SECURITY AWARENESS

CONTENTS

1.INTRODUCTION....3
2.PROTECTING YOUR COMPUTER & DATA....3
3.PHISHING AWARENESS....3
4.ONLINE BANKING LOG IN DETAILS TIPS....4
5.IMPORTANT INFORMATION....4

1. INTRODUCTION

MeDirect is committed to keeping your personal information secure and confidential. To help preserve your personal information you must also take an active role. Here is some information about security tips and guidelines:

2. PROTECTING YOUR COMPUTER & DATA

Install and update an anti-virus software.

Virus protection software is critical to keeping your personal computer and your Online Banking safe. Install and regularly update anti-spyware, anti-virus and firewall protection on your computer. Scan your computer often for all types of viruses including those that could be used to capture keystrokes.

Be cautious with downloads.

Do not download software from unknown or untrusted websites unless you are sure it is safe.

Be cautious of email attachments and URL links.

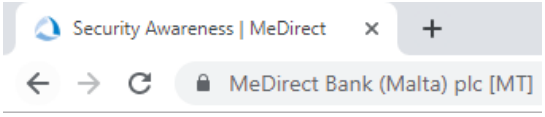
Do not open email attachments received from unknown sources. Never access your bank website through a URL link in an email, even if the email appears to have come from your bank. Type the web address into your browser yourself.

Regularly install updates and patches.

Make sure your computer operating system and web browser software are always updated with the latest updates and security patches. This ensures that you close the gaps in the system that viruses or other malware could exploit.

Lookout for the secure padlock.

The login pages of our website are secured through an encryption process, so a locked padlock or unbroken key symbol should appear in your browser window when accessing our login pages.



Regularly clear your cache, cookies and browsing history.

Consider deleting your browser's cache and your browsing history after each session, or on a periodic basis, so that any account information and browsing history are removed completely.

Log out.

When your online banking is complete log out before closing the browser or going to the next website. Always log out and close the browser every time you leave your computer.

3. PHISHING AWARENESS

What is phishing?

Phishing is a fraud used by cyber criminals who imitate legitimate banking/financial organisations through emails. Cyber criminals use this technique to obtain personal information including login credentials. Victims are persuaded to provide these details either by logging on to fraudulent websites or – less frequently – by phone or fax.

How do you recognise a phishing email?

Awkward greeting.

A phishing email may address the customer with a generic greeting ("Dear valued customer" or something similar) rather than by name.

Spelling and bad grammar.

Cyber criminals are not renowned for correct grammar and spelling. If you notice spelling and grammatical mistakes in an email, it is most likely a phishing email.

"Click on this link".

If you see a link in a suspicious email message, do not click on it. The link looks official, but when your mouse cursor rolls over it the link's source code points to a completely different website. Remember that you can always type a URL into your web browser instead of clicking on a link. Similarly, never use a phone or fax number contained within an email without first checking its authenticity using our website.

Urgent call to act.

Different approaches include things such as "We're updating our records", "We've identified fraudulent activity on your account", or

"Valuable account and personal information was lost due to a computer glitch". To encourage people to act immediately, the email usually threatens that the account could be closed or cancelled.

Have you received a suspicious email?

If you receive a suspicious email, SMS (text message) or any other suspicious message that claims to be from MeDirect:

- Do not respond to the email or SMS.
- Do not open any attachments or click on URL links contained in the email.
- Call us on **+356 2557 4400**. The information you provide will be used to help reduce fraud online.
- Forward the email to phishing@medirect.com.mt for us to investigate.

4. ONLINE BANKING LOG IN DETAILS TIPS

You are responsible for maintaining your Online Banking log in details.

Create unique log in details every time.

Stay away from anything easy to guess and anything connected to your life. Avoid using birth dates, birth years, family members or pet names, information related to your school or college or favourite team, account numbers, or other easily obtained information.

Follow the "8 4 Rule".

It is recommended that you use passwords that are at least eight characters in length. The more characters in the password the better. Any password should contain at least one of the following – lower case letter, upper case letter, a number and a special character, but it cannot contain whitespace.

Use different log in details.

That way, if someone does get access to one of your web or bank accounts, he or she cannot access the rest of them.

Change your log in details on a regular basis.

Schedule a recurring appointment on your calendar to change your credentials once every six months.

Do not type your log in details on a computer that does not belong to you.

If possible, do not use someone else's computer that you do not trust to login to any website, especially for very sensitive purposes such as banking.

Keep your log in details secret.

Do not carry your log in details in your purse or wallet and if you write them down, keep them somewhere safe, and not near your computer. Make sure no one watches you access your Online Banking platform.

Do not share with anyone.

Anyone includes your friends and family.

5. IMPORTANT INFORMATION

Be wary of anyone asking you to disclose personal and log in details. Remember:

- MeDirect staff will **never** ask for your log in details or any other personal or financial information except to verify your identity when you have asked us to do something.
- The MeDirect website **will not** ask you to enter any of your security details except on webpages that can be accessed directly from the home page of our website.

If you have any reason to believe that you may have been the victim of a phishing fraud or that your account with MeDirect has been fraudulently used, call us immediately on **+356 2557 4400**.