The Information Security Policy Statement

The Information Security Policy ensures that:

- Confidentiality, integrity and availability of information systems in tax and revenue administration is preserved.
- All applicable requirements, including those pertaining to the information security aspects will be complied with.
- Objective of ensuring information security, the effectiveness of the Information Security Management Systems will be improved continually.
- Information security objectives are set based on the Information Security framework.

Beware of cybercriminals

MRA continuously updates its security measures to protect your tax transactions. However, cybercriminals are after your data, your devices, your accounts and your information all have tremendous value to them. Thus they make use of different attack vectors to meet their objectives at all cost. Once they have been able to access your system they will execute different attacks namely:

Username & Password harvesting

They will install software to capture your keystrokes gather sensitive information such as usernames and password to access your online accounts such as banks to steal or transfer money, cloud services and access your sensitive information.

Identity theft / Identity hijacking

They can steal your online identity to commit fraud or sell your identity to others, such as: your social media account, email account or any other accounts.

Contact/email harvesting

They can read all your emails, access your contacts and sell the information to competitors.

Extortion

They take over your device and demand money to decrypt it. They may take pictures and videos of you and demand payment so as not to release same.

Botnet

Your device will form part of an entire network of hacked computers controlled by the cybercriminals which may be used to attack other systems by launching Denial of service or sending spam to millions of people.

What can be done?

Nevertheless, the attack surface can be reduced by taking the following measures:

- Ensure automatic update is enabled on your device and you install latest updates for the operating system and applications running on your device for legitimate sources.
- Install security software on your devices and ensure you continue to keep your security software updated and run regular checks to maintain security levels on your devices.
- Avoid using public wireless networks since if not secured properly you are vulnerable to someone using it to get to your information.
- Keep a backup of all your information in a secure location away from your computer.
- Limit sharing personal information on the internet and social sites.

Email attacks - Scams / Phishing / Spear phishing

You can be a phishing target at work or at home.

Phishing is a psychological attack used by cyber criminals to trick people into giving information or taking an action.

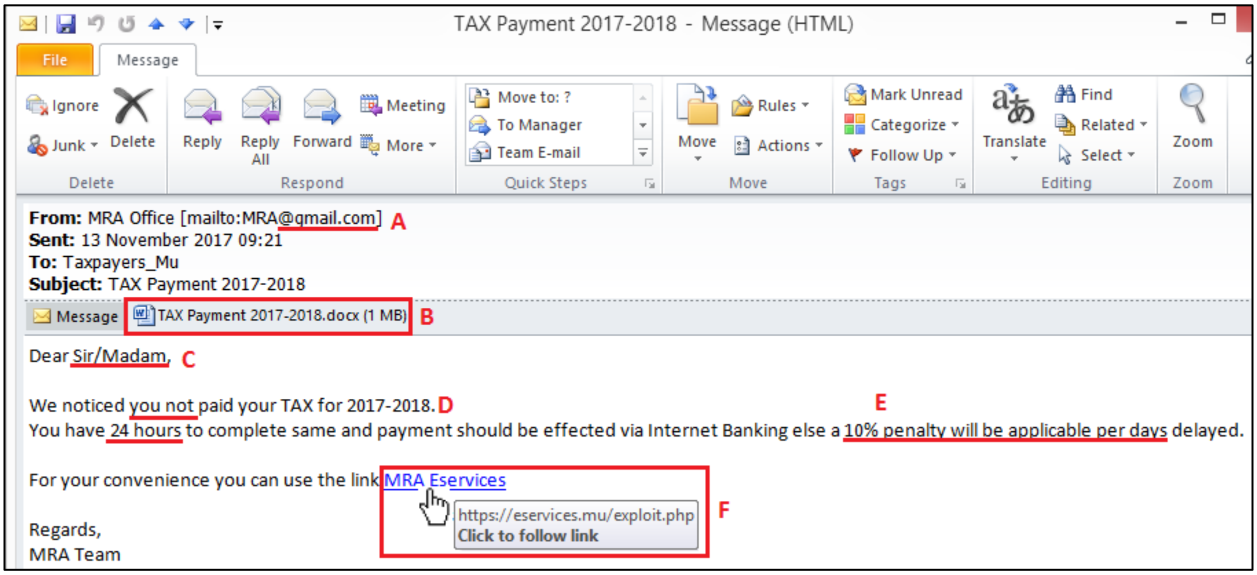
Spear phishing is same as Phishing but targeting specific person.

MRA stakeholders are randomly emailed with false “spoofed” emails made to look as if these emails were sent from MRA, but are in fact fraudulent emails aimed at enticing unsuspecting taxpayers to part with personal information such as bank account details or install malware on their devices.

These emails contain links to false forms and fake websites made to look like the “real thing”, but with the aim of fooling people into entering personal information such as bank account details which the criminals then extract and use fraudulently.

If you identify suspicious email coming from MRA report same to MRA via the Hotline.

How to identify a suspicious email:



From: MRA Office [mailto:MRA@gmail.com]
Sent: 13 November 2017 09:21
To: Taxpayers_Mu
Subject: TAX Payment 2017-2018

Message | TAX Payment 2017-2018.docx (1 MB)

Dear Sir/Madam,

We noticed you not paid your TAX for 2017-2018.
You have 24 hours to complete same and payment should be effected via Internet Banking else a 10% penalty will be applicable per days delayed.

For your convenience you can use the link MRA Eservices

https://eservices.mu/exploit.php
Click to follow link

Regards,
MRA Team

A. Check the email addresses properly. If the email appears to come from MRA, but the ‘FROM’ address is someone’s personal account such as @gmail.com or @hotmail.com, etc., this is most likely to be email spoofing. Also check the “TO” and “CC” fields to verify if the email was sent to people you do not know or do not work with. In such situation, do not reply, flag it as spam and contact MRA to report the issue.
B. Be apprehensive of attachments and their contents only open those you are expecting.
C. Be suspicious of email addressed to the general “Dear Customer or Dear Sir/Madam”. Ask yourself if you are expecting an email from MRA?
D. Be suspicious of any grammatical or spelling mistakes.
E. Be wary of any email requiring “immediate action” or creating a sense of urgency.
F. Be careful with links only click on those you are expecting. Also, hover your mouse over to confirm the true destination of the link.

What to do if you receive suspicious communications from MRA

1. Suspicious email claim to be from MRA

- Do not reply
- Do not open attachments as they may compromise your device
- Hover on the link check the destination before clicking
- Forward the mail to CERT-MU and advise MRA.

2. Phone call, someone claiming to be from MRA

- MRA call will come from +230 207 6000 other numbers are likely to be suspicious
- Note the Caller name, phone number and other identifying details
- Do not disclose sensitive information like passwords, bank details, etc… over the phone
- Call MRA and confirm if the Caller was an employee of MRA.

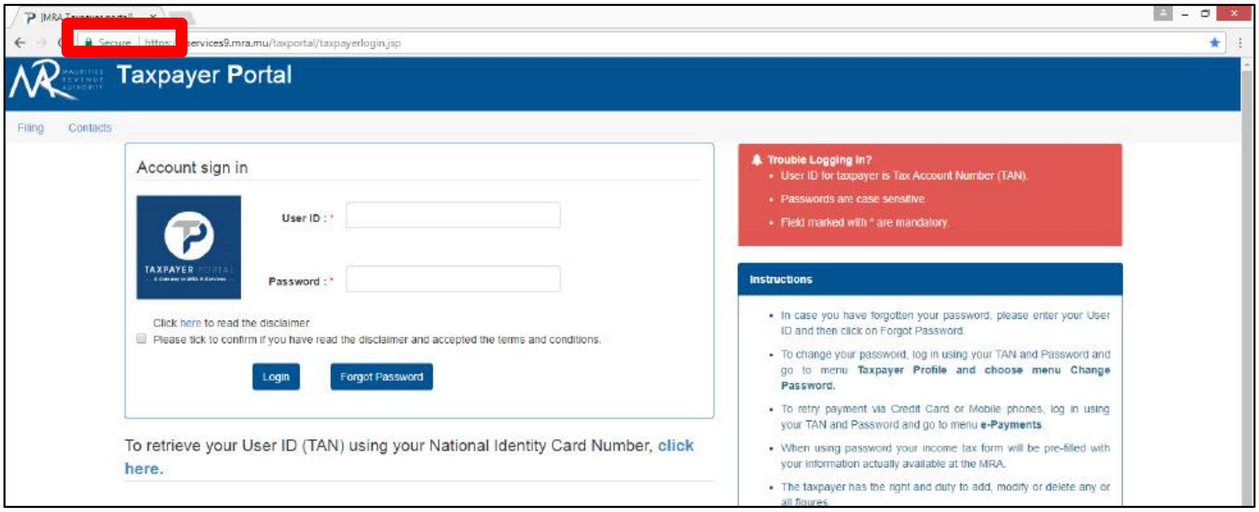
3. Letters or Fax claiming to be from MRA

- Check MRA website to see if there is any related information regarding the letter / Fax.
- If you cannot find such information call MRA to confirm if the letter / fax are legitimate.

Protect against identity theft and identity fraud

1. MRA will never request your banking details in any communication that you receive via post, email, or SMS. However, for the purpose of telephonic engagement and authentication purposes, MRA will verify your personal details. More importantly, MRA will not send you any hyperlinks to third party websites - even those of banks.

2. While accessing MRA Electronic services ensure it is a secure website; same can be identified as per below:
   - Ensure the link is http**s.** S is secure.
   - Verify the certificate ensure it is valid. If it is green it is fine else report the issue to MRA.



[MRA Taxpayer portal]
Secure | https://services9.mra.mu/taxportal/taxpayerlogin.jsp
MAURITIUS REVENUE AUTHORITY
Taxpayer Portal
Filing
Contacts
TAXPAYER PORTAL

Account sign in

User ID : *

Password : *

Click here to read the disclaimer

□ Please tick to confirm if you have read the disclaimer and accepted the terms and conditions.

Login Forgot Password

To retrieve your User ID (TAN) using your National Identity Card Number, **click here.**

Trouble Logging In?

- User ID for taxpayer is Tax Account Number (TAN).
- Passwords are case sensitive.
- Field marked with * are mandatory.

Instructions

- In case you have forgotten your password, please enter your User ID and then click on Forgot Password.
- To change your password, log in using your TAN and Password and go to menu **Taxpayer Profile and choose menu Change Password.**
- To retry payment via Credit Card or Mobile phones, log in using your TAN and Password and go to menu **e-Payments**.
- When using password your income tax form will be pre-filled with your information actually available at the MRA.
- The taxpayer has the right and duty to add, modify or delete any or all figures

3. Never share your user ID, password with anyone.
4. Protect your tax documents and other financial documents are kept in a secure place.

5. Do not Access MRA Eservices from emails access same from MRA website: http://www.mra.mu/
6. Make use of Cross-cut shredder, pulping or burning to destroy sensitive documents.
7. Tighten up on your social networking security settings. Criminals can use this information to impersonate you.

Password management

Username and passwords are allocated to taxpayers to have controlled access to MRA Eservices and ought to be used under strict and controlled conditions. The password management best practices are:

- **All username and password allocated to taxpayers should be kept confidential**. Passwords should not be revealed to anyone, including stakeholders.
- Avoid creating passwords based on guessable information such as birth dates, phone numbers, family names and pet names.
- Memorise your passwords and do not write them down or store them anywhere.
- Avoid common letter or number patterns in your passwords such as ‘123’ or ‘abc’.
- Do not allow browsers to save your passwords.
- All taxpayers should abide to the security information published on the MRA website in order to preserve the integrity and confidentiality of MRA Eservices.

Non-conformance to the above security measures represents a breach to the **Computer Misuse and Cybercrime Act 2003** as per **Section 8. Unauthorised disclosure of password**.

If you suspect that your password has been used by someone else, change it and notify MRA immediately.

Social Engineering

Be aware of what you share on social media. You should limit the amount and type of identity information you post on social networking sites as information can easily be shared, even outside of your network. Adjust your privacy settings to control the amount and type of information you want to share to ensure your profile is only accessible to those you trust. Be aware of whom you are interacting with online and only share information with people you know and trust. Hackers can access and obtain your personal information (Full name, date of birth, address, TAX Account Number, bank account details, license details, passport details etc.), and can use these to attempt to commit fraudulent activity, so be vigilant in the protection of your personal information.

System Management

Systems should be managed in such a way to minimise attack surface of the different systems forming the network.

Ensure the following are in place:

- Systems are configured per configuration standards – CIS, NIST, OWASP, etc…
- All default usernames, passwords and other vendor default settings should be changed.
- Systems are patched regularly; the earliest possible.
- Only business justified services are run on the systems all other unnecessary services should be disabled.
- Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.
- Audit logging should be enabled to detect any anomaly.
- Implement a process to immediately detect and alert on critical security control failures
- All systems must be protected from unauthorized access from untrusted networks

Query

If you have any query on the above, please contact MRA Hotline on +230 207 6010