MAURITIUS CIVIL SERVICE MCSMAA LTD ASSOCIATION LTD

ONLINE ACCESS SECURITY INFO

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Your e-services experience needs a safe and secure environment and for that, the Mauritius Civil Service Mutual Aid Association Ltd (MCSMAA Ltd) has deployed security measures to reduce your exposure to certain types of fraud. You also have your part to play to ensure that your online activity is secure. The protection of your privacy matters to us. Be assured that our services rely on high-security mechanisms to protect your finances. Your collaboration is key, remember to take some precautions too.

2.0 WAYS TO KEEP YOURSELF SAFE

2.1 Feel the ease of safe e-Services by observing some simple practices.

2.1.1 Key security tips to keep your e-Services safe:

- Check that the web address is what you were expected. The safest way to have access to the site is to click on the MCSMAA Ltd website m.c.s.mutualaid@intnet.mu and log in from there.
- Always log out your MCSMAA Ltd e-services session and close your browser when you have completed your transactions.
- Never access MCSMAA Ltd e-services from a link in an e-mail or from redirections from other websites - genuine emails from MCSMAA Ltd will **NOT** contain any links to our e-services.
- Never provide sensitive information in response to any e-mail, even if the e-mail looks like it comes from a genuine financial institution like MCSMAA Ltd. No MCSMAA Ltd staff will ask you for your e-services credentials.
- Never respond to e-mails that request personal and financial information and never click on a link in such e-mails! This may take you to a spoof website. MCSMAA Ltd will never ask you to fill out any survey in exchange of money or ask you to provide your account number so that you can be rewarded. It's best that you delete suspicious e-mails.
- Don't leave your computer, smartphone or tablet unattended when you are connected to MCSMAA Ltd e-services.
- Never change security details such as your password in a public place like a Cybercafé.
- Monitor your account activity regularly for any unusual transactions and notify the MCSMAA Ltd immediately if you suspect any discrepancies. It is one of the best ways to safeguard yourself against fraud.

3.0 STAY ALERT

3.1 Some common signs that your computer might be malware-infected.

- It's running extremely slow.
- Applications/Programs won't start and won't work properly.
- Your computer runs out of hard drive space and crashes.
- You cannot connect to the Internet.
- You get pop-up ads, unusual messages and unsolicited pages that display on screen.
- Your friends are getting strange messages from you.
- Files have been deleted.
- You are locked out of your computer.
- You cannot shut down your computer.

Remember: If you suspect any malicious software lurking on your computer, stop doing any e-services transaction!

Using safely your smartphone

- Protect your phone with a password and an antivirus.
- Always ensure that your apps are from reputable sources.
- Never store passwords on your phone.
- Make sure you log-off after every session on e-services.
- Remember to inform us whenever your contact details change.
- Check your browser for the lock symbol which indicates that you are using a secure and reputable web connection.

4.0 REPORT IT

4.1 Hoax emails are continually in circulation. Although they might appear genuine, they are fraudulent!

Tips to Spot a Fraudulent Email...

- Those request sensitive personal information.
- They invoke a sense of urgency or make use of threatening language.
- They request information confirmation and update.
- They have spelling mistakes.
- They have odd-looking email even if the display name might look correct.

If you receive an email that appears to be from MCSMAA LTD but looks suspicious, forward it to us immediately at m.c.s.mutualaid@intnet.mu

Remember: Under no circumstances you should act on those suspicious emails.

5.0 MORE SAFETY TIPS TO KEEP YOU SAFE ONLINE

5.1 Before using e-services, make sure the site you're accessing is legitimate.

- Ensure that the website you are visiting is genuine and secure, prior making a payment or share sensitive information.
- Look at the URL of the website in your browser's address bar. If it starts with 'https://', it means that the site is using a SSL Certificate and is hence secured. The SSL Certificate secures the information.
- Look for a closed padlock icon in the address bar; it indicates encryption is being used on the web page. The icon is located on the left of the URL on most recent browsers, but may vary in location on older ones.
- If you reach a website and get a warning that the site cannot be trusted, it might be an indication of forgery. We recommend not to submit any private information through. If the website is owned by a reputable company, validate this behavior with them. We also encourage you to look out for poor grammar or spelling on sites and check that the design is consistent as this may be an indication of forgery.

5.2 Protect your password

Your passwords are the keys to your personal and financial information. Don't let them fall in malicious hands.

Malicious people are always lurking to sneak into your devices and get hold of your accounts. Your passwords are valuable so make sure to protect them. We've compiled a few tips to help you safeguard your password.

Don't use the same passwords for different applications, and especially don't share same password for e-services and social networks applications such as Facebook, LinkedIn, etc.

- Never disclose your password to anyone.
- Do not keep your passwords on yourself.
- Memorise your passwords.
- Do not write them down or store them anywhere.
- Change your password regularly.

- If you suspect that your password has been compromised, notify MCSMAA Ltd immediately.
- Don't allow any website to store your password.
- Never send your passwords by email.

5.3 Keep your mobile phone secure

Increasingly you rely on our mobile phones to browse, bank, shop, socialise and more. Make sure no one has access to it.

The more you rely on your smartphones to run your lives, the more you are exposed to security risks. It's key that you keep your mobile gear secure and take simple precautions so to protect your confidential data.

- Protect your device with a passcode and/or fingerprint detection - it's your first line of defense. Enable your phone's automatic passcode lock feature, and still remember to lock it when not in use.
- Use Apple's Find my iPhone or Google's device manager for Android™, to help you locate your phone and wipe the data should it fall into the wrong hands.
- Equip your device with an anti-virus software and keep it updated.
- Keep your Operating System and Apps up-to-date - this will make sure you have the latest security patches.
- Install a security software on your phone, if available.
- If you change your mobile phone number recorded at MCSMAA Ltd or you lose your mobile, contact the MCSMAA on +230 213 6060. We recommend that you ensure that we always have your most current contact information so we can contact you if we notice any unusual activity on your accounts.
- Keep your mobile clear from text messages from MCSMAA Ltd - especially before sharing, discarding or selling your device.
- Never disclose any personal details via text message (password, account numbers, etc.).
- Use Secured Networks whenever possible - they are password-protected.

5.4 Stay safe when using social networks

- Chances are social networking has become an integral part of your online activities. You may use it to stay in touch with friends, family and businesses, share experiences and content, and its potential is growing. But, with these remarkable capabilities come several risks. Hackers use the same opportunities in an environment where guard is relatively low to boost their

existing acts – distribute malwares, gather your personal information and more.

- Be wary of any unusual posts. Be skeptical about what you read online, criminals may post misleading information to make you feel deceptively confident.
- Be cautious when providing your personal information on social networking sites, as remember that, the more information is available about you online the easier it is for fraudsters to steal your identify. Personal Information could also serve social engineering attacks to target people - often young ones - to meet them in person, which could lead to life threatening situations. Increasingly, social media is being used by malicious people to track potential victims' whereabouts.