

## GENERAL INFORMATION SECURITY GUIDELINES

Banque BEMO SAL is committed to minimizing the risks of using online services, and has invested in adequate systems and processes to protect you when using our network. **Online security is a shared responsibility.** As your options for banking online grow, so does your need to safeguard your privacy and security while using the internet on your personal computer, tablet or mobile device. **This brochure is to help you understand what you should do to minimize these risks including general guidelines on protecting your information and assets.**

### PROTECTING YOURSELF AND YOUR IDENTITY

The Bank will never ask you to provide the below through e-mail, mobile applications, social media platforms or any other digital communication means:

- Passwords
- Account Numbers
- Card Numbers
- User Names
- Any other confidential or private customer information

Fraudulent e-mails may be designed to appear as though they were originated from Banque BEMO SAL, therefore:

**-Don't respond to e-mails that claim to be from your bank (or any other company) requesting your account details.** No bank is ever likely to approach you this way

**-Be careful about what (and where) you click online.** Keep in mind that links you receive in emails or in messages on social networking sites can be harmful or fraudulent, even if they appear to come from friends. Requests for personal information or a call for immediate action are almost always a scam. If you suspect the link might give you a virus or steal personal data, don't click on it. Talk to the sender directly and make sure it came from them.

**-Be mindful of how much personal information you share on social networking sites.** The more you post about yourself, the easier it might be for someone to use the information you post to access your accounts, steal your identity and more. Maximizing your privacy settings on social networking sites can also help protect your personal information.

### KEEP YOUR COMPUTER PROTECTED

- 1) Protect your devices with a comprehensive endpoint security solution that includes antivirus, anti-malware, and firewall protection. Ensure the endpoint security solution is always up-to-date.
- 2) Perform regular scans of your systems for malware and other risks.
- 3) Operating system providers such as Microsoft, periodically releases updates and patches that improve the security of your operating system. You should periodically check for these updates and keep your system current or configure it to do so automatically.
- 4) Use strong, unique passwords for all your accounts. A strong password should be at least 12 characters long and include a mix of uppercase letters, lowercase letters, numbers, and symbols. Avoid using easily guessable information like your name, birthday, or common words. Consider using a password manager to help you create and store strong passwords. **Change passwords every 90-180 days unless there is a suspected compromise.**
- 5) Disable the auto complete function in your browser, which can store or retain user IDs and passwords that can be used by others.
- 6) Do not open email attachments or click on links from strangers. Delete junk or chain emails. Watch out for file extensions and delete any files that have double extensions, as they are likely to be a virus. Do not install software or programs of unknown origin in your PC. Before you run any software or program, ensure that it comes from a trusted source.
- 7) Always log off from your online session when you leave your computer unattended, even for a short while, and clear your browser cache after logging off.

## ADDITIONAL SECURITY MEASURES

- 1) Enable Multi-Factor Authentication (MFA) whenever possible, especially for your online banking account. MFA adds an extra layer of security by requiring a second verification method, such as a code sent to your phone, in addition to your password.
- 2) Avoid accessing sensitive information or accounts on public Wi-Fi networks. Use a VPN to encrypt your traffic when connecting to public Wi-Fi.
- 3) Keep your mobile operating system updated. Use a strong PIN or biometric lock. Be cautious about installing apps from unknown sources and review app permissions. Enable "find my device" features.
- 4) Encryption protects your data, both in transit and at rest, from unauthorized access. Our bank uses encryption to safeguard your information on our online banking platform.
- 5) Be aware of your surroundings when using ATMs. Shield the keypad when entering your PIN and check for skimming devices.
- 5) Be extra vigilant about protecting your accounts from unauthorized access. AI can be used to generate realistic phishing attempts and social engineering attacks. Enable multi-factor authentication (MFA) whenever possible.
- 6) Scammers are increasingly using AI to create more sophisticated and convincing scams. Be wary of unsolicited offers, requests for personal information, or any communication that seems too good to be true.
- 7) AI models are not always accurate and can sometimes generate biased or misleading information. Always double-check information from AI sources and use your own judgment.
- 8) Be aware that the data you provide to AI services might be retained indefinitely. Understand how to delete your data from these services, if possible.
- 9) AI Impersonation: Be aware that AI can be used to impersonate individuals. If you receive a suspicious communication that appears to be from someone you know, verify its authenticity through a separate channel (e.g., a phone call).

## ARTIFICIAL INTELLIGENCE AWARENESS: PROTECTING YOUR INFORMATION WHEN USING AI TOOLS

- 1) Never share personal, financial, or health information with AI models. These models are often trained on vast amounts of data, and there is a risk that your information could be stored, used, or shared in ways you do not intend. Consider any information you input into an AI as potentially public.
- 2) Be aware that AI can be used to create convincing fake content, including phishing emails, social media posts, and even audio and video deepfakes. Always verify information from unfamiliar sources, even if it seems legitimate.
- 3) If you choose to use AI tools, carefully review their privacy policies to understand how your data will be collected, used, and protected.
- 4) AI models can provide helpful information, but they are not a substitute for professional advice. Always consult with qualified experts for financial, medical, or legal guidance.

Please report directly to [bemo@bemobank.com](mailto:bemo@bemobank.com) any suspicious calls, e-mails, messages or if your online-banking username or password were stolen. Our staff and management have pledged to apply all the necessary measures to insulate your confidential information and to give you the directions needed on how you can protect yourself from the diversified risks and threats; however, your awareness and application of the aforementioned steps and guidelines remain **ESSENTIAL** in helping us secure your information.