UMTB
MIZRAHI TEFAHOT BANK LTD

How to Prevent Fraud

Safeguard your Social Security Number.

- Never provide your Social Security Number unless you have initiated the contact and have confirmed the business or person’s identity.
- Do not use your full or partial Social Security number as a personal identification Number (PIN) or a password.
- If you must provide a Social Security number in an email or on a Website verify that it is encrypted, and be sure that the recipient will protect it.
- Do not record your Social Security number on a check, traveler’s check, gift certificates, etc., unless required by law.
- Do not carry your Social Security card and be cautious of your surrounds when disclosing your Social Security Number.

Eliminate Paper

- Reduce the amount of mail and paper with your personal information printed on it to reduce the chance of criminals stealing it.
- Stop receiving paper account statements and canceled checks. View and download them online instead.
- Sign up for direct deposit to have your funds put directly into your account without paper checks.

Secure Your Computer

- Anti-spyware and anti-virus protection detects and removes viruses and spyware that can steal vital information.
- A firewall prevents unauthorized users from gaining access to a computer, or monitoring transfers of information to and from the computer.
- Operating system and software updates, sometimes called “patches” or “service packs,” should be installed as soon as possible.
- Web browser updates are deployed with your security in mind so keep them current.

Types of Online Fraud

Phishing and Spoofing

Sometimes criminals may send you email that looks like it has come from UMTB-LA. These phony emails ask you to go to a Website that also looks like UMTB-LA and provide your personal account information. These emails may even ask you to call a phone number and provide account information. But the Website is a fake.

- **Asking for personal information** should raise a flag since UMTB-LA emails will never ask you to reply in an email with any personal information, such as your Social Security number.
- **Urgent appeals** claim that your account may be closed if you fail to confirm, verify or authenticate your personal information. UMTB-LA will not ask you to verify information in this way.
- **Messages about system and security updates** claim that the bank needs to confirm important information due to upgrades and state that you must update your information online. UMTB-LA will not ask you to verify information in this way.
- **Offers that sound too good to be true** often are. You may be asked to fill out a short customer service survey in exchange for money being credited to your account, and you are then asked to provide your account number for proper routing of the supposed credit. You should never give your account number unless you have full knowledge of the credentials of the survey party.
- **Typos and other errors** are often the mark of fraudulent emails or websites. Be on the lookout for typos or grammatical errors, awkward writing and poor visual design.

To protect against phishing and spoofing:

- Make sure you are at UMTB-LA's Website when you sign in to Online Banking
- If you receive a suspicious email, do not click on any links or reply to it. Simply delete it.
- To report a suspicious email that uses UMTB-LA's name, you can forward it to info@umtbusa.com.

Money Mules

Money mules are unsuspecting victims who become middlemen for criminals trying to launder stolen funds. Victims are lured by the promise of a new career opportunity making large sums of money for minimal work. Criminals recruit money mules, send them stolen money and then ask the money mules to wire or transfer the money unwittingly to the criminals. Using the money mule masks the criminal's identity.

The money mule may keep a commission for performing the transfer or wire. The victims of these scams may not only have their bank accounts closed and financial reputation ruined, but are often left financially responsible for returning the stolen funds.

Common signs of a money mule scam:

- **Overseas companies** requesting money transfer agents in the US
- **Opening new bank accounts** to receive money from someone you don't know
- **Accepting large sums of money** into your personal bank account for a new job
- **Transferring or wiring funds** out of your personal bank account to people you do not know

Malware

Malware, short for "malicious software," includes viruses, spyware and trojans that are designed to infiltrate or damage a computer system. Malware is often used to steal personal information and commit fraud. There are several easy ways to minimize the risk of malware:

- **Downloads** from file sharing and social networking sites can be distributions points for malware
- **Attachments and free software** from unknown sources shouldn’t be opened or installed
- **Pop-up advertisements** asking for personal or financial information are likely fraudulent, so it's better to close them
- **Updated security and system software** can protect your computer from malware threats

Vishing

Vishing uses Voice over Internet Protocol (VoIP) to call, leaving an automated recording. It alerts the consumer that their account has experienced unusual activity. The message instructs the consumer to call the same phone number shown in the spoofed caller ID with the same name as the financial company they are pretending to represent. And sometimes, criminals who try to get consumers to turn over personal data send emails and text messages containing fraudulent phone numbers.

Rather than provide any information, you should contact UMTB-LA at the customer service number you normally use to verify the validity of the message.

Types of Mobile Fraud

Fake Mobile Banking Apps

Criminals may develop and publish fake mobile banking applications attempting to steal your Online Banking credentials. Here are tips for recognizing an unofficial bank application:

- The developer or author of the application is not the bank
- The application is being promoted on a third party site, somewhere other than the official application store for your mobile device
- There is a charge for downloading the application—Banks do not currently charge for mobile application downloads

To help protect your accounts and information, don't download or install a bank’s Mobile Banking App if you spot any of these warning signs.

Currently, UMTB-LA does not offer Mobile Banking.

SMShing

SMShing is phishing that happens via SMS text message. A criminal sends a text messages tricking you into replying with financial or personal information or clicking on links that will sneak viruses onto your mobile device. To guard against these scams:

- Don't respond to a text message that requests personal or financial information.
- Verify the phone numbers that appear in a text message. Store UMTB-LA’s phone numbers in your mobile contacts for a quick cross-check. Or, you can go to the Contact Us page.

Currently, UMTB-LA does not offer SMS text message service.

Stolen Devices

Mobile phones and tablets offer convenience, but they’re also easy to lose or steal, which can put your information at risk.

- Password-protect your device so it can’t be accessed unless the password is entered
- Enable an automatic screen-locking mechanism to lock the device when it’s not actively being used
- Consider using a remote wipe program, this will give you the ability to send a command to your device that will delete any data
- Keep a record of the device's make, model and serial number in case it's stolen

Traditional Online Threats

Viruses, malware and other programs that steal your personal information or financial details are also able to infect some mobile devices.

- Some tablets may support traditional anti-virus products. Consider installing an anti-virus program if supported on your device
- Back-up the device's data. This will allow you to restore the data if you need to wipe the memory to remove a harmful software threat

Stay vigilant about security when taking advantage of the convenience these devices offer.