Safeguarding Your Finances

At Agility Forex Ltd. we prioritize the security and integrity of every transaction you make with us. We are committed to providing you with reliable and efficient money services, but equally important is empowering you, our valued client, with the knowledge and tools to protect yourselves from the pervasive threats of fraud, scams, and cybercrime.

The financial landscape is constantly evolving, and unfortunately, so too are the methods employed by criminals. While we leverage state-of-the-art technology and rigorous compliance protocols to safeguard our systems, your awareness and vigilance are crucial layers of defense. This notice outlines the common risks you may face and, more importantly, how you can proactively protect your hard-earned money and personal information when using our services.

Common frauds, scams and cybercrimes to be aware of:

Investment Fraud
The leading fraud in terms of dollar loss, often involving cryptocurrency or fake online investment platforms, promising high returns with little to no risk. Sometimes referred to as 'Pig Butchering', these scams often pressure victims to send money quickly. The scammers may provide access to a fake trading platform or app, where the victim can see their investments seemingly growing. Finally, when the victim attempts to withdraw their funds, the scammer will create excuses or disappear with the victim's money. In 2024, over $310 million was lost to investment scams.

Romance Scams
Scammers build virtual relationships to gain trust and affection. Fraudsters will often start by asking to borrow a small amount of money for a fabricated emergency, health, family, business or investment issue, which they immediately repay. They will continue this pattern, increasing the amount of the 'loan' or 'gift' until a large sum has been transferred, at which point the fraudster will disappear without trace. Canadians lost over $58 million to romance scams in 2024.

Money Mules
A money mule is an individual who is approached by fraudsters to act as an intermediary for transferring stolen or illicit funds.

Account Takeovers (ATOs)
Gaining unauthorized access to a victim's online accounts to make fraudulent transactions or steal identity. This is a direct threat to your funds held with any financial institution.

Phishing/Smishing/Vishing (Impersonation Scams)
These are perhaps the most pervasive. Fraudsters impersonate legitimate entities (CRA, banks, law enforcement, even our MSB, etc.) via email, text, or phone calls to trick victims into revealing sensitive information or sending money. Always verify the sender!

Emergency/Grandparent Scams
Callers pretending to be a loved one in distress (e.g., arrested, in an accident) needing urgent money. These often lead to requests for money transfers because of the immediate pressure and emotional manipulation.

Tech Support Scams
Fraudsters claiming to be from well-known tech companies, asserting a computer problem, and demanding payment for "fixes" or access to the device.

Phishing/Social Engineering
The foundational tactic for many cybercrimes, using deceptive tactics to trick individuals into revealing sensitive information or performing actions that compromise security. This is often the precursor to other cyberattacks.

Identity Theft
Stealing and using a person's identity information (e.g., name, SIN, banking details) for fraudulent purposes, which can lead to unauthorized access to financial accounts, including those with MSBs.

Vendor Impersonation Scams
Corporate clients are highly susceptible to Business Email Compromise (BEC) and vendor impersonation scams, where criminals pose as legitimate suppliers or business partners requesting payment changes.

Examples:

Vendor Impersonation: A fraudster hacks the account of one of your vendors. They use the corporate email and impersonate the CFO of the vendor and send an email asking you to change their banking information for payments.

Phishing leading to Account Takeover: You receive an email that appears to be from your bank, asking you to "verify account information" due to a "security update." The email has a link that leads to a fake website designed to look exactly like the online banking page. You enter username and password. The credentials are immediately stolen by the cybercriminals. Within hours, they use the stolen credentials to log into your bank account and initiate several unauthorized money transfers before you notice the suspicious activity.

How you can protect yourself:

1. Be Skeptical and Verify Everything

- Unsolicited Contact: Be extremely wary of unexpected calls, emails, or messages, especially if they demand urgent action or personal information. Remember, legitimate organizations, including us, will never ask for your passwords or full banking details via unsolicited communications.
- Verify Identity: If someone claims to be from any official entity, hang up and call them back using a phone number from the official website or a trusted, publicly available source, not a number they provide.
- Pressure Tactics: If you feel pressured, it's a major red flag. Take your time, ask questions, and consult a trusted friend or family member if you're unsure.
- Romantic Interests Online: If a new online acquaintance quickly professes love, avoids video calls or in-person meetings, and soon asks for money, be extremely suspicious.

2. Guard Your Personal and Financial Information

- Think Before Sharing: Never share bank account details, credit card numbers, Social Insurance Numbers (SINs), or other sensitive information with unverified individuals or websites.
- Secure Online Accounts: Use strong, unique passwords for all your online accounts, especially those linked to financial services. Consider using a reputable password manager.
- Enable Multi-Factor Authentication (MFA): Wherever possible, enable MFA for an extra layer of security on your Agility Forex account and other critical online services. This typically involves a second verification step, like a code sent to your phone, in addition to your password, making account takeovers much harder.

3. Recognize Common Scam Red Flags

- Demands for Specific Payment Methods: Scammers frequently insist on payment via wire transfers or cryptocurrency, as these methods are difficult to trace and recover. Legitimate businesses rarely demand these payment forms.
- Offers That Seem Too Good to Be True: If an investment opportunity promises unusually high returns with little to no risk, or a prize notification requires an upfront fee, it's likely a scam.
- An offer to make money quickly and with little effort.
- Requests to register a company and a business bank account.
- Employment duties limited to opening accounts and receiving and sending money.
- Employment offers and other communications poorly written and include spelling mistakes and grammatical errors.
- Unusual Account Activity: Be vigilant for signs of an account takeover, such as password reset notifications you didn't request, unrecognized transactions, or emails in your sent folder that you didn't send.

4. Be Cyber-Savvy

- Keep Software Updated: Ensure your computer, smartphone, and other devices have the latest security patches and operating system updates. These updates often include crucial security fixes that protect against known vulnerabilities.
- Antivirus/Anti-malware Software: Install and regularly update reputable antivirus and anti-malware software on your devices.
- Be Wary of Links and Attachments: Do not click on suspicious links or download attachments from unknown or unexpected emails/messages. They can contain malware designed to steal your credentials or compromise your system.

If you believe you have been a victim of, or an attempt has been made against you, report it!

How to Report Fraud to the Authorities:

- **Canadian Anti-Fraud Centre (CAFC)**:
  - Online: https://www.antifraudcentre-centreantifraude.ca/report-fraude-eng.htm
  - Toll-free: 1-888-495-8501
- **Local RCMP Detachment:** Find the contact information for your local RCMP detachment on the RCMP website
- **Consumer Protection BC**
  - Telephone: 604-320-1667
  - Toll Free: 1-888-564-9963
  - Email: info@consumerprotectionbc.ca
- **Credit Bureaus:** If personal information or identity is compromised, contact:
  - **Equifax Canada:** 1-800-465-7166
  - **TransUnion Canada:** 1-800-663-9916

By adopting these proactive measures, you can significantly reduce your vulnerability to fraud, scams, and cybercrime, ensuring a safer and more secure experience when utilizing the services of Agility Forex Ltd. Remember, your vigilance is your strongest defense, and we are here to support you.