RICHTER GUARDIAN

RGSA 08-28-23-01
Date: August 28, 2023

BMO Scam Highlighting Vulnerabilities in Two-Factor Authentication

INTRODUCTION

A recent article published by CBC news highlighted a concerning scam that involved the Bank of Montreal (BMO). The scam managed to exploit vulnerabilities associated with the two-factor authentication (2FA) system of the bank. This advisory aims to provide an overview of the issue, its implications, and recommendations.

SUMMARY OF INCIDENT

The scam primarily targeted customers with lines of credit. Perpetrators pose as bank employees and use a combination of phishing techniques and flaws in the 2FA process to gain unauthorized access to customers' accounts, subsequently making unauthorized transactions.

IMPLICATIONS

1. The trustworthiness of 2FA is at stake. Customers generally perceive 2FA as a robust security measure, but this incident underscores potential vulnerabilities.
2. The scam demonstrates that even with the second layer of authentication, user accounts can be compromised if the process isn't foolproof.
3. Potential loss of customer trust in banking institutions due to such vulnerabilities.

RECOMMENDATIONS

1. Stay Informed: Regularly update oneself about the latest scams and phishing techniques. Always be skeptical of unsolicited calls or emails asking for personal or banking information.
2. Use Advanced Security Features: Wherever possible, use advanced security features like biometric authentication or hardware-based security keys.
3. Monitor Accounts: Regularly check bank accounts for unauthorized transactions and report any discrepancies immediately.
4. Stay Educated: Participate in security awareness sessions provided by your Richter Guardian team, the bank or other trusted organizations.

HOW RICHTER GUARDIAN CAN HELP YOU

While 2FA is an essential security feature, it is not infallible. Richter Guardian clients should be proactive in understanding its limitations and continuously seek ways to enhance their security posture.

- Call us anytime you are unsure. If you receive a call from someone purporting to be your bank and you are unsure, call us to help you determine the legitimacy of their communication.
- Schedule a one-on-one call with our analyst to review the two-factor authentication security measures that may be available to you through your bank.

RICHTER GUARDIAN

RGSA 08-28-23-01
Date: August 28, 2023

Table 1 – Levels of two-factor authentication that may be available to protect your bank account.

Type of 2FA Method	Description	Level of Strength of Security
SMS-Based 2FA	Sends a one-time code to the user's registered mobile number, which they then input to authenticate.	**Moderate** - Vulnerable to SIM swapping attacks and interception.
Push Notification (e.g., through an app)	Sends a notification to the user's registered device, prompting them to approve or deny the login request.	**High** - More secure than SMS-based, but can still be vulnerable if the device is compromised.
Token-based Authenticator (e.g., Google Authenticator, Authy)	Uses a time-based one-time password (TOTP) generated by an app. The user enters the code displayed on the app.	**High** - Not vulnerable to SIM swapping; however, a device compromise could pose risks.
Hardware Tokens (e.g., YubiKey, RSA SecurID)	Physical device that generates or holds digital authentication data. Some require a button press to display a code, while others transmit the code when plugged into a device.	**Very High** - Not susceptible to most common cyber-attacks. Loss or theft of the device is the primary concern.
Biometric 2FA	Uses the user's unique physical or behavioral characteristics, such as fingerprint, face recognition, or voice pattern.	**High** - Difficult to replicate but isn't immune to all attacks (e.g., high-quality replicas or recordings). Also, concerns about data privacy persist.
Email-Based 2FA	Sends a one-time code or link to the user's registered email address, which they then use to authenticate.	**Moderate** - Security depends on the strength and security of the user's email account. Vulnerable to email hacking.

CONTACT US

Have a quick question? Send us an email.
Email: support@richterguardian.com

Phone number: +1 844.908.3950
Monday to Friday 9 a.m. to 5 p.m. (Eastern Time)

Need assistance upgrading your device?
Schedule a session with us by clicking here or by using this link:
https://calendly.com/richter-guardian/upgrade-assistance