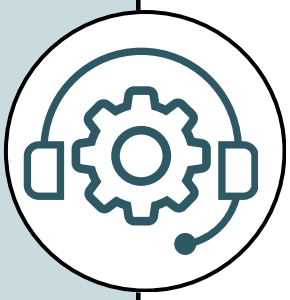
How is Multifactor Authentication Being Bypassed by Scammers?

Multifactor authentication is a crucial element of cybersecurity designed to safeguard important online accounts. Below are examples of online banking scams that show how criminals have evolved their tactics to deceive individuals into revealing their one-time passwords or compromising their devices and personal information.



Remote Access Tech Support

A fraudster may use social engineering tactics to trick a victim into downloading a remote desktop application under the guise of solving a problem. For example, an elderly person received a call from someone claiming to be from their telecom provider, stating that their internet was slower than it should be. Believing this, the member allowed remote access to their computer, which was then locked. The criminals used the browser's saved passwords to access the member's credit union account, bypassing multifactor authentication since it was a trusted device.

Fraudulent e-transfers via Facebook Marketplace

A common scam targeting credit union members involves fraudulent e-transfer payments, often in response to a Facebook Marketplace advertisement. The scammer pretends to buy an item and sends an email resembling a legitimate Interac e-transfer. The member is prompted to click a link or scan a QR code, leading to a spoofed webpage where they enter their credentials and a one-time code. This allows the fraudster to access the account, make unauthorized transactions, and change account information, while flooding the member's email with notifications to cover their tracks.

Compromised Email as a second factor

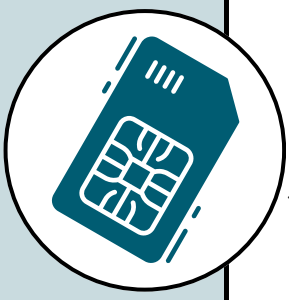
Often, members are unaware of how their device was compromised until an examination reveals the presence of spyware and other malware. This could be due to visiting malicious websites, clicking bad links, or other means. Fraudsters can then obtain banking credentials and access the member's email inbox. If the second factor for authentication is a one-time code sent to the email, the fraudster can retrieve the code, thereby bypassing multifactor authentication.

Vishing "Credit Union Employee" calls

When a member's online banking credentials have been compromised and all that remains is for the fraudster to retrieve the one-time code, fraudsters have called the member and posed as a credit union employee aiming to secure their account. The fraudster tells the member that they are calling due to suspicious activity and will send them a code to reset their online banking. The member believes the fraudster and provides their code over the phone.

Call Centre Fraud - Member Impersonation

In call centre fraud, the initial point of compromise is often unknown, but fraudsters already possess the member's online banking credentials and enough information to pass verification. They impersonate the account holder and request a phone number change from the call centre agent. Once the number is updated, the fraudster receives one-time passcodes and can make unauthorized transactions.



SIM Card Swap - Telecommunications Fraud

A fraudster may bypass multifactor authentication through a SIM swap or eSIM swap. By gathering enough personal information, they can impersonate the victim and request a transfer from the phone carrier. For instance, a victim might receive a text appearing to be from their telecom provider, asking them to confirm their identity. To ensure it wasn't a scam, the victim followed instructions to enter an authentication code sent by the actual telecom provider into the chat with the fraudsters. This allowed the SIM swap to be finalized, enabling the fraudsters to receive all calls and text messages, including one-time passcodes for online banking.

KCCU is here to help in your fight against fraud

In today's fast-paced digital world, fraud is an ever-present threat that can affect anyone, anywhere. KCCU is dedicated to helping you stay protected against these dangers by offering a range of tools and resources to safeguard your financial well-being. From advanced security measures to educational programs, KCCU provides comprehensive support to ensure your personal information remains secure and your financial transactions are safe.

In addition to technological safeguards, KCCU places a strong emphasis on educating its members about fraud prevention. KCCU empowers you with the knowledge needed to recognize potential scams and take proactive steps to avoid them. With KCCU by your side, you can confidently navigate the digital landscape, knowing that you have a trusted ally in the fight against fraud.

KCCU
Kingston Community Credit Union

Kingston Community Credit Union is here for you.
If you have concerns that you or someone you know is the victim of a scam or fraud please let us help.
www.kccu.ca or call us at 613-384-5555