Account Takeover Prevention & Recovery

An account takeover (ATO) is serious business. It occurs when a cybercriminal gains access to your online account and uses it to withdraw or transfer money, make purchases, or extract additional information that they can sell or use to access other accounts. For the purposes of this blog, we'll be discussing financial ATOs, but others can involve email and social media accounts, and government benefits, too.

An ATO is not only damaging to your finances, but it's also harmful to your sense of well-being. And unfortunately, there is no absolute failsafe protection against it. However, there are steps you can take to limit your vulnerabilities and stop ATO fraud if it occurs. Maintaining strong account security and remaining vigilant are key. So, how do you protect your online accounts?

Use strong passwords and change them regularly. Strong passwords contain a combination of uppercase letters, lowercase letters, numbers, and special characters. Passwords should not contain any information that can easily be found on your social media pages, like your birthday or the name of your dog. Instead, they should be random. For example, look outside, what do you see? Pair that with the time of day to create a complex password like M@pleTree0743. Ideally, you should have a unique, secure password for every online account, no matter the type. Do not repeat passwords, either. For example, if your current online banking password is Spr!ng1234, don't change it to something similar like Spr!ng5678. Create a new password that's unique and very different from previous passwords and other accounts. Fraudsters are more successful with their attacks if you're using the same passwords for multiple accounts. And, it should go without saying, but don't share your passwords with anyone!

Utilize multifactor authentication. When available, enable multi-factor authentication for all of your online accounts. Multi-factor authentication sends a verification code via email or text message upon account login. You must enter this code along with your username and password as an extra step in verifying your login credentials.

Monitor email and text message communication. This tip is two-fold. First, watch for email or text message notifications regarding any change made to your online account. Cybercriminals may alter account information like your email address, phone number, or even your physical address in order to withdraw or transfer your money. Even if they can overcome your authentication measures, the sooner you're able to detect a compromised account, the better chances you'll have in minimizing risk and preventing further damage.

You should also monitor your communications for phishing attempts. Phishing is the practice of sending fraudulent emails or text messages claiming to be from reputable companies in order to persuade you into revealing personal information, such as passwords and account numbers. It's important to monitor your emails and text messages and investigate any embedded links. Go directly to the institution or company website instead of clicking on the provided links. This will help identify and block phishing attempts. When in doubt, contact the institution or company that supposedly sent the email or text message in question to verify its validity. **Note that Emerald Credit Union will never contact you via email, text message, or phone call requesting personal identification or account information.**

As stated above, even with strong account security and vigilance, there is no 100% protection against an ATO. So, what should you do if you experience an ATO?

Cease all activity on devices that may be compromised. This includes desktop and laptop computers, cell phones, tablets, and smart watches. Disconnect the affected device(s) from any network connections to isolate the operating system from remote access.

Contact your financial institution and take the following actions. Request assistance where needed:

- Disable online access to your accounts.
- Change your online banking username and password.
- Close the affected accounts and open new ones as appropriate.
- Review all recent transactions and authorizations on the affected accounts.
- Confirm that no one has requested an address, email, phone number, or PIN change, ordered a new debit or credit card, checks, or other account documentation to be sent to a different address.
- Submit any paperwork your financial institution may require to report the takeover, determine financial losses, and begin the possible recovery process.

File a police report. Provide the facts and circumstances surrounding any financial loss. Make sure to obtain a copy of the police report, which should include the report number, date, time, department, location, and the name of the officer who took it. The police report may initiate a law enforcement investigation, with the goal of identifying, arresting, and prosecuting the offender, and possibly recovering financial losses.

Please note that the above is for informational purposes and is not intended to provide legal advice.