Is Your Account Compromised? Recognize the Signs and Learn What Steps to Take

Published 10/28/2024 by Giuseppe Aloisi

There are various clues and signs that can suggest the possibility that someone has taken over your online account. Seemingly urgent or suspicious requests can be phishing attempts designed to trick you into giving away your personal information. These threats often prey on your instinct to act quickly, like changing passwords or responding to requests, which can play right into the hands of cyber attackers. It's crucial to always verify before taking any action online.
Let’s break down three common indicators of compromised accounts, using examples you may encounter as a Seneca student or employee. This will help you better recognize potential threats and protect yourself more effectively.

Passwords

If one day you find that your Seneca account password isn’t working and suspect it’s been changed without your knowledge, don’t panic. Here are some steps you can take:

1. Reset your password: Attempt to regain access by resetting your password.
   - Note: This works unless the attacker has changed your recovery email.
2. Contact ITS: If resetting your password doesn’t work, reach out to the ITS Service Desk immediately to report the issue - they can help you secure your account and prevent further misuse.
3. Check notifications: Monitor your email and other possible security measures that indicate any unsolicited changes to your password.

Pro Tip: Implementing Multi-Factor Authentication (MFA) can prevent situations like this. While MFA adds a strong layer of security, it’s important to remain vigilant, as it too can be exploited if not used properly.

Account Activity

Understanding your account activity is crucial in identifying potential compromises. However, it can be very confusing, especially when it varies based on the devices you use and your travel locations. Monitoring your activity through MFA apps is an effective way to verify if your account has been misused.

Seneca students and employees can easily monitor their activity through their Microsoft Authenticator or Duo MFA apps. Here's what you can do:

1. **Check login details:** The MFA apps provide information such as the operating system, location, browser, and apps used during the suspicious login time.
2. **Suspicious login detected:** If you notice a suspicious login on your Seneca account ensure to cross check it using the factors listed above. A suspicious login can be in identified using various methods, some of the examples include:
   - A login attempt from a different location.
   - A login attempt that uses a different device than what you would use.
   - A login attempt that uses a different operating system.

This feature is particularly useful for reviewing and confirming account activities when suspicious logins occur, helping you verify and identify potential compromises.

Unsolicited Changes to Security Measures

It can be challenging to monitor every change that happens to your account. However, security measures such as MFA play a crucial role as the last line of defence. Therefore, it is essential to make sure that these security measures work as they should.

- Signs of Unauthorized Access: Unsolicited changes indicate that your account might be compromised.
- Increased Vulnerability: Not paying enough attention to unsolicited changes like the above could potentially open channels for cyberattacks.

Examples of unsolicited changes include:

- Disabled MFA: The removal of your MFA setup can leave your account vulnerable.
- Recovery Email Modified: If you notice your recovery email has been altered without your knowledge, it's a serious red flag.

Always ensure your security measures, especially MFA, are active and functioning to protect your account from unauthorized access.

Summary

In today’s digital age, safeguarding your online accounts is more critical than ever. Recognizing the signs of a compromised account, such as unexpected password changes, suspicious login activities and unsolicited security measure modifications, is the first step in protecting your personal information. By staying vigilant and utilizing tools like MFA to monitor account activity, we can significantly reduce the risk of unauthorized access. Proactive measures and prompt actions are your best defence against potential threats.

According to the Government of Canada here are some of the best ways to stay Cybersafe:

- Use unique and complex passwords.
- Implement as many security options as you can to ensure that your social media and email accounts are secure.
- Back up sensitive information and know where you have it backed up.
- Remember to stay updated no matter what platform you seem to be using.
- Keep an eye out for phishing messages that can be sent to you by anyone.