Frequently Asked Questions Multi-Factor Authentication (MFA)

As part of the University's enhanced security measures, Multi-Factor Authentication (MFA) is now required for all users with a UB email address to better protect accounts and information. What is MFA? It's a simple extra step that keeps your account secure by verifying your identity in two ways—first with your password, and then with a one-time code sent to your phone or another device. Students, faculty, and staff now need to use MFA to access the UB email, Microsoft 365 applications, Moodle, Innosoft Fusion (for the Wellness Centre), and the Online Computer Library Centre (OCLC).

Here are answers to some frequently asked questions to help make this transition as easy as possible.

1. Q: My phone does not have sufficient storage for MFA, so what happens now?

A: No problem! You can clean up (remove) unused apps, old files, photos and documents to accommodate the Microsoft Authenticator. Otherwise, contact the Technology Services Helpdesk for assistance.

2. Q: With MFA, will the University now have access to my personal details and information and be able to track me?

A: No, the University cannot access your personal details, track your activity, or monitor your phone. Using an authenticator app such as Microsoft simply generates one-time passcodes, valid for 30 seconds, and does not collect personal data beyond the app itself.

3. Q: Given the recent ransomware incident, if I use my phone for MFA, will it expose me to a cyber-attack?

A: MFA is designed to protect you, not expose you. It adds an extra layer of security, making it significantly harder for attackers to access your account—even if they have your password.

4. Q: Can my phone be cloned once MFA is on it?

A: No, using MFA does not increase the risk of your phone being cloned. It simply sends verification codes or prompts to confirm your identity.

5. Q: What if my personal device breaks or is lost, how will I access my account?

A: If this happens, contact the Technology Services Helpdesk immediately. Temporary access solutions can be provided, and your MFA can be reset on a new device.

6. Q: Can I use something other than a cell phone to authenticate my account?

A: Yes, you can use an authenticator app on a tablet.

7. Q: Do I need data or internet connection to use the MFA?

A: Yes, an internet connection is required to install the authenticator app that generates the codes online.

8. Q: Why are we using MFA and not some other security feature?

A: MFA is one of the strongest and most effective ways to protect your account from unauthorized access. Passwords alone can be compromised, but MFA provides an additional layer of security to keep your data safe. Following international security standards is really important for business continuity and data protection.