Create a Strong Password

Password rules every MOS employee must follow

A weak password is an open door. This guide explains MOS password requirements and shows you how to create strong passwords you can actually remember - plus how to use a password manager.

Jean Claude Munyakazi | IT Systems Administrator | Magister Operis Systems

🏢 COMPANY POLICY

MOS Password Policy §3.2 requires:

- Minimum 12 characters
- At least 1 uppercase letter
- At least 1 number
- At least 1 special character (! @ # $ %)
- Password must be changed every 90 days
- Cannot reuse the last 5 passwords
- Never share your password with anyone, including IT

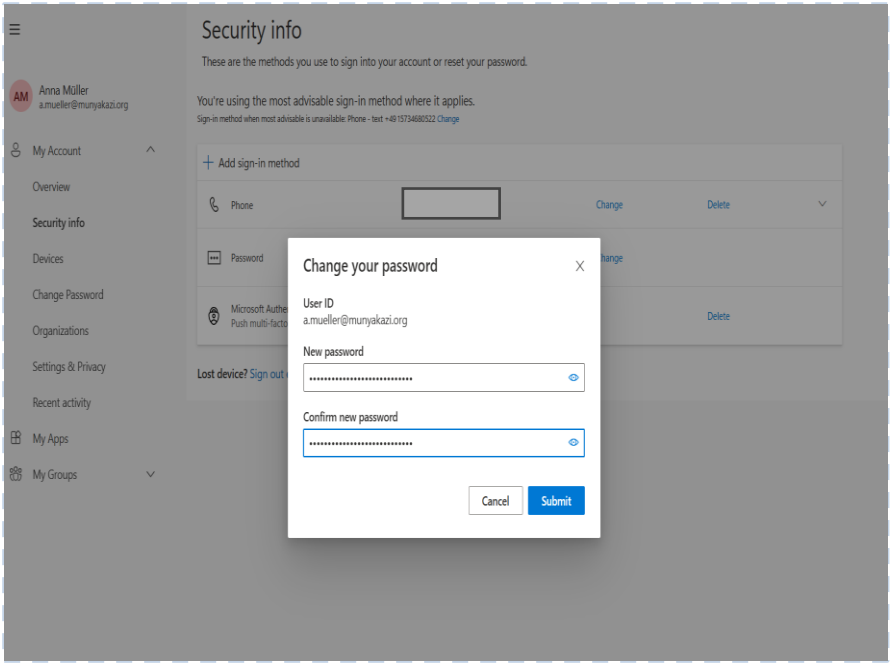
⚠️ WHY THIS MATTERS

Weak passwords are the #1 cause of data breaches worldwide. A 6-character password can be cracked in seconds. A 12+ character password takes hundreds of years.

If your account is compromised, attackers can access company emails, files, and client data, and you may be held responsible.

STEP 1

Build a Strong Passphrase



INSTRUCTIONS

The easiest way to create a strong memorable password is a passphrase:

1. Think of 4 random words: Coffee-Mountain-River-Lamp

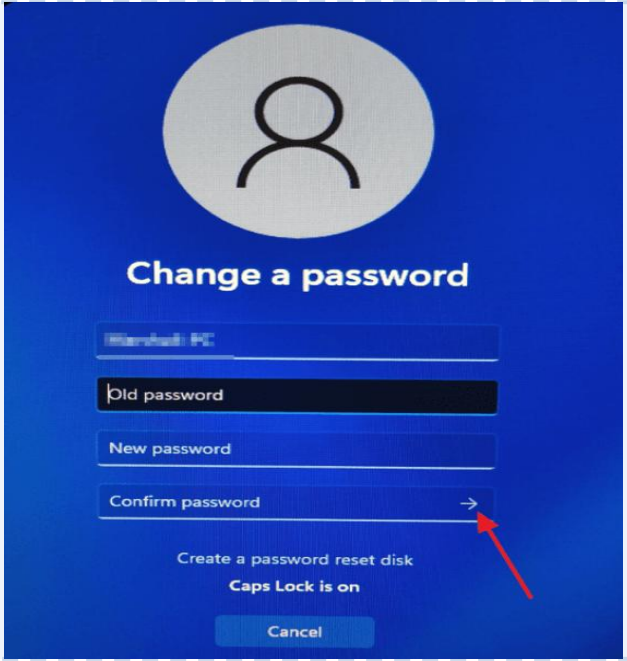
2. Add a number and special character: Coffee-Mountain-River-Lamp7!

3. This is 30 characters, extremely strong, easy to remember

→ Never use: your name, birthday, company name, or sequences like 12345

STEP 2

Change Your Windows Password



INSTRUCTIONS

1. Press: Ctrl + Alt + Delete

2. Click: Change a password

3. Enter your current password

4. Enter your new strong password twice

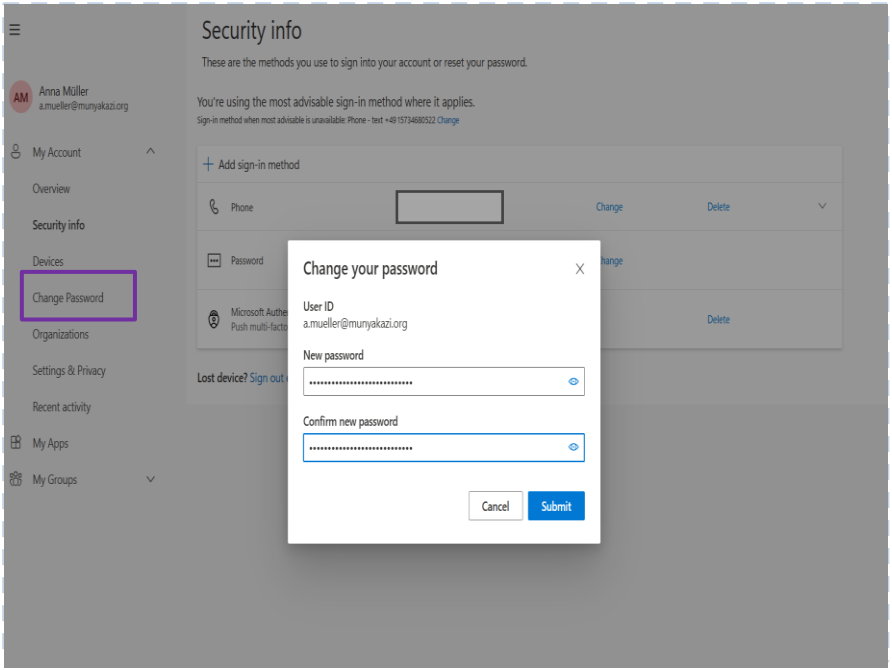
5. Press the arrow button or Enter

→ Your Windows login password is now updated

Note: Your M365 password may be separate, check Step 3

STEP 3

Change Your M365 Password



INSTRUCTIONS

1. Go to: myaccount.microsoft.com

2. Click: Password (left menu)

3. Enter current password, then your new password twice

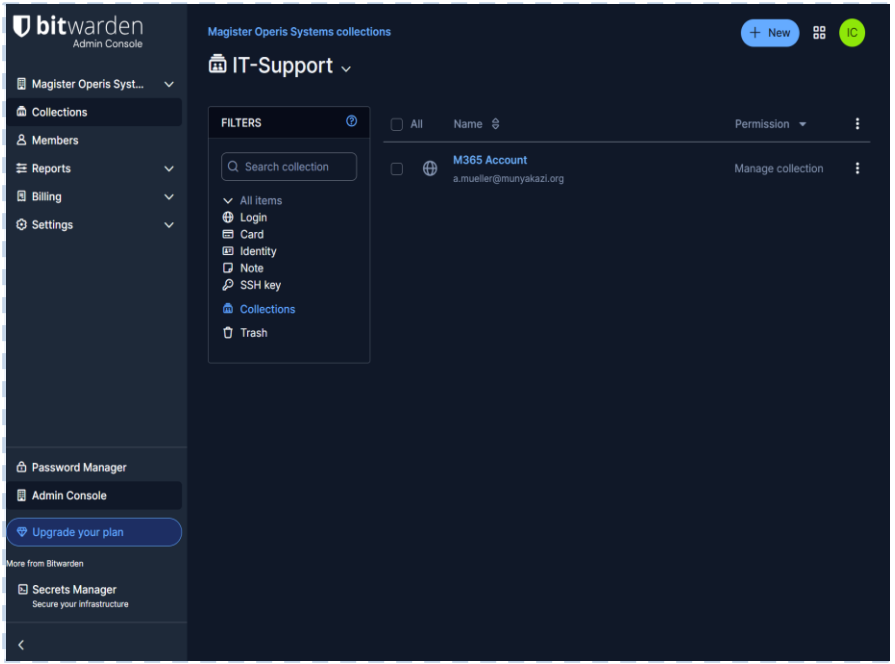
4. Click: Submit

→ Your company email and M365 apps are now protected

If you use the same password on other sites, change those too

STEP 4

Use a Password Manager (Optional but Recommended)



INSTRUCTIONS

A password manager remembers all your passwords so you only need to remember ONE master password.

1. Recommended: Bitwarden (free) - bitwarden.com

2. Create a free account with a very strong master password

3. Install the browser extension

4. Save each password as you change them

→ The manager auto-fills passwords when you visit sites

❌ What NOT To Do

❌ Don't reuse passwords across sites

If one site is breached, attackers try your password everywhere. Each account needs its own unique password.

❌ Don't use obvious personal information

Name, birthday, department, company name, attackers try these first.

❌ Don't write passwords on paper or sticky notes

Post-it notes on your monitor are visible to anyone who walks past your desk.

❌ Don't ignore the 90-day reset reminder

You will receive an email reminder. Ignoring it will result in your account being locked.

❌ Don't share your password with colleagues

Even with trusted colleagues. If something goes wrong, you are accountable for actions under your account.

❌ Don't store passwords in browser without protection

Browser-saved passwords are at risk if your computer is accessed without your knowledge.

Need Help? Contact IT

IT Helpdesk Chat

Teams → MOS IT Support
Channel: Incidents

Email Support

itsupport@munyakazi.org
Response within 4 hours

Urgent Security Issue

Call your manager immediately
Do NOT wait for email response

Remember: IT will NEVER ask for your password over email, chat, or phone.

✅ Quick Summary

Create a Strong Password

1. Use a passphrase of 4+ random words with numbers and symbols
2. Minimum 12 characters, never use personal info
3. Change Windows password: Ctrl + Alt + Delete → Change a password
4. Change M365 password at myaccount.microsoft.com → Password
5. Use a password manager like Bitwarden to manage multiple accounts
6. Never share your password, not even with IT staff