MOS USER SECURITY GUIDE

Guide #005

Safe Internet & Email Use

Protecting company data online and on company email

Every website you visit and every email you send from your company account represents MOS. This guide covers safe browsing habits, company email rules, and what to do on public WiFi.

Jean Claude Munyakazi | IT Systems Administrator | Magister Operis Systems

munyakazi.org

🏢 COMPANY POLICY

MOS Internet & Email Policy §6.1:

- Company devices must not be used for personal social media
- Do not send confidential data via personal email
- Public WiFi requires a VPN if accessing company systems
- Do not download software without IT approval
- Company email must not be used to sign up for non-work services
- All email communication must be professional in tone

⚠️ WHY THIS MATTERS

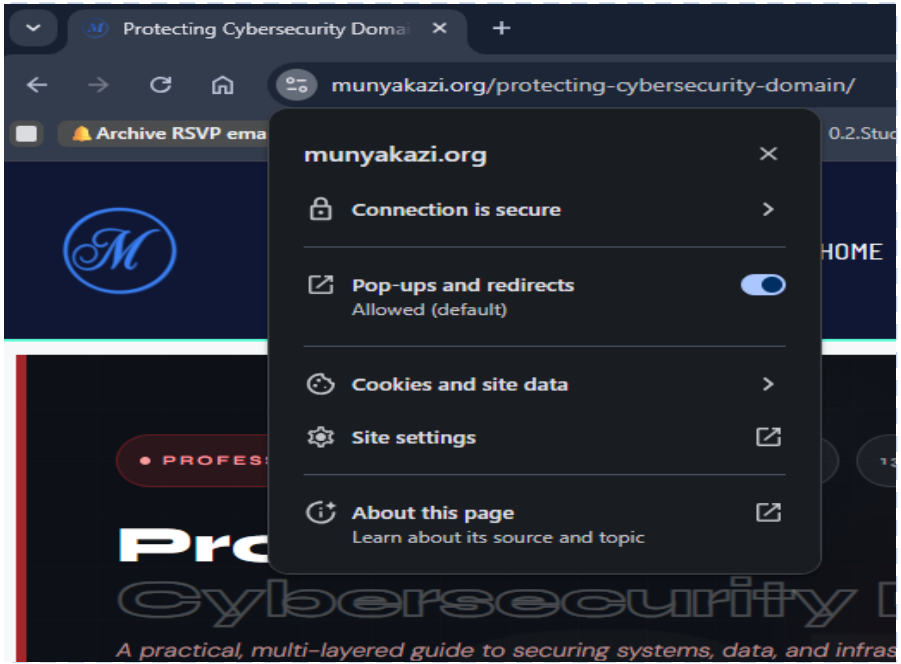
Your company account and device are connected to the MOS network. Unsafe browsing habits can:

- Introduce malware to the entire company network
- Cause data leaks of confidential client information
- Create legal liability for the company

When you use company equipment, your activity represents MOS professionally and legally.

STEP 1

Safe Browsing on Company Devices



INSTRUCTIONS

On your company computer:

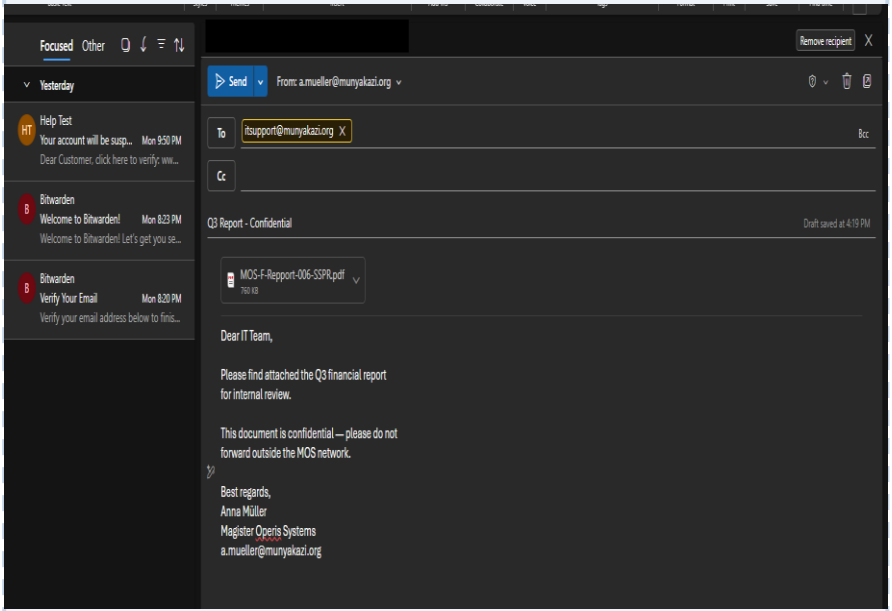
✅ Stick to work-related websites during work hours
✅ Check that websites use HTTPS (padlock icon in browser)
✅ Download files only from official, known sources
✅ Keep your browser up to date (IT manages this)

❌ Avoid: streaming sites, personal social media, online shopping
❌ Never install browser extensions without IT approval
❌ Never bypass security warnings in your browser

→ If a website feels wrong, close it and contact IT

STEP 2

Using Company Email Correctly



INSTRUCTIONS

Your company email (yourname@munyakazi.org) is for work only:

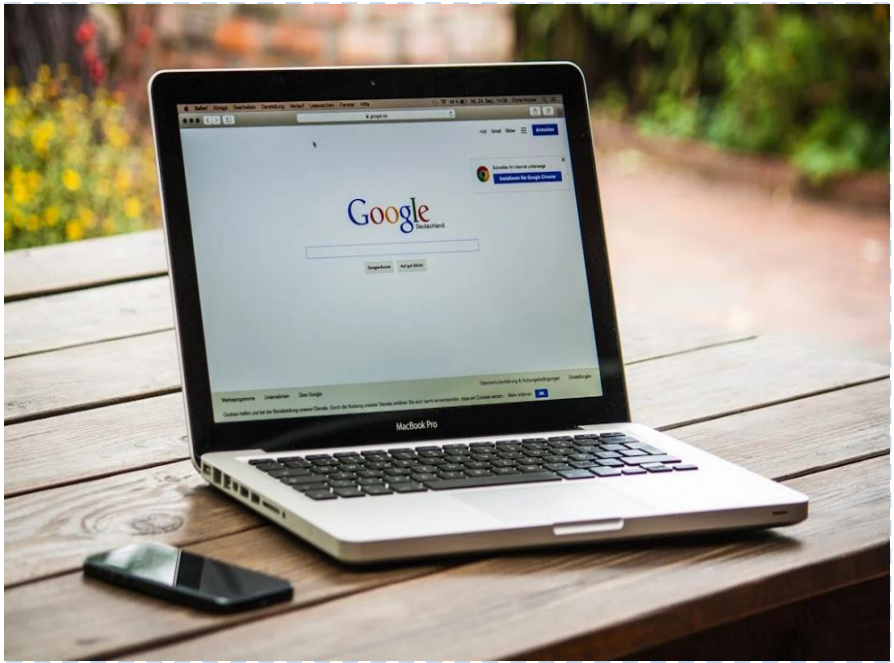
✅ Use it for all work communication
✅ Keep tone professional; emails can be forwarded
✅ Confirm recipient before sending sensitive information

❌ Never send confidential files to personal email addresses
❌ Do not sign up for newsletters or personal services
❌ Do not auto-forward company email to personal accounts
❌ Never send passwords, account numbers, or PINs by email

→ Company email is monitored and retained for 90 days

STEP 3

Public WiFi Safety



INSTRUCTIONS

When working from a café, airport, or hotel:

⚠️ Public WiFi is NOT secure, anyone on the same network can see your traffic

1. Connect to the MOS VPN before accessing any company system
   → Ask IT for VPN setup instructions if needed

2. Avoid accessing banking or sensitive personal accounts

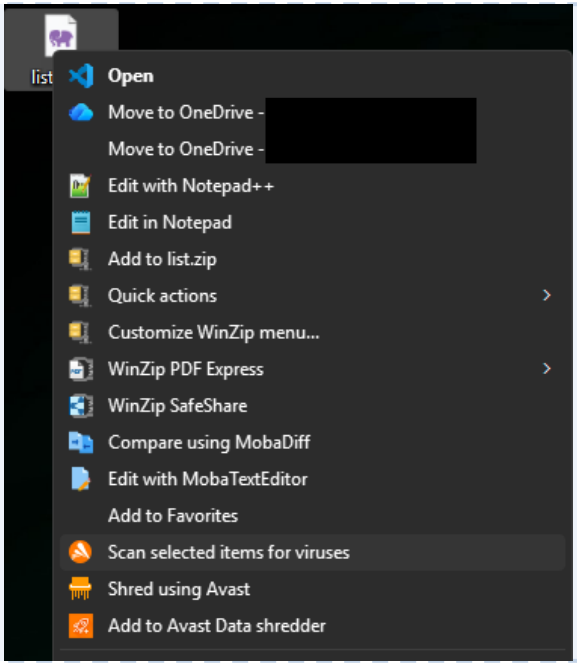
3. Use your phone's mobile hotspot as a safer alternative

4. Log out of all accounts when finished on a public device

→ Never access company systems on public WiFi without VPN

STEP 4

Downloading Files and Software Safely



INSTRUCTIONS

Before downloading anything on a company device:

1. Ask yourself: is this download necessary for work?

2. Software must be approved by IT before installation
   → Submit a request via Teams: MOS IT Support channel

3. Files from emails should be scanned:
   → Right-click the file → Scan selected items for viruses before opening

4. Only download from official websites (.gov, .com companies you know)

5. Never run .exe files from unknown sources

→ When in doubt; ask IT first, download later

What NOT To Do

Don't send company files to personal email

Even for convenience. This bypasses company security controls and may violate data protection law.

Don't use company email for personal subscriptions

This exposes your company address to spam, marketing lists, and potential data breaches at third parties.

Don't connect to public WiFi without VPN

All company system access on public networks requires the MOS VPN. Ask IT for setup if you don't have it.

Don't ignore browser security warnings

'Your connection is not private' warnings exist for a reason. Close the page and report it to IT.

Don't install software without IT approval

Unapproved software can contain malware and void IT support for your device.

Don't leave sessions open on shared computers

Always log out completely from all company accounts on any shared or public computer.

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

Safe Internet & Email Use

1. Use company devices for work-related websites only
2. Company email is for work only; never forward to personal accounts
3. Always connect to MOS VPN before using public WiFi
4. Never download software without IT approval; submit request via Teams
5. Scan downloaded files with Windows Defender before opening
6. Log out of all accounts when finished on a shared or public device