MOS USER SECURITY GUIDE

Guide #006

What To Do If You're Hacked

Incident response steps every MOS employee must know

If you suspect your account or device has been compromised, acting quickly is critical. This guide gives you the exact steps to take in the first 30 minutes of a suspected security incident.

Jean Claude Munyakazi | IT Systems Administrator | Magister Operis Systems

🏢 COMPANY POLICY

MOS Incident Response Policy §7.1:

- All suspected security incidents must be reported to IT within 30 minutes
- Do not attempt to fix the issue yourself before contacting IT
- Do not delete evidence; do not format or wipe your device
- Document what happened (time, what you clicked, what you noticed)
- Cooperation with the IT security investigation is mandatory

Failing to report an incident promptly may worsen the breach.

⚠ WHY THIS MATTERS

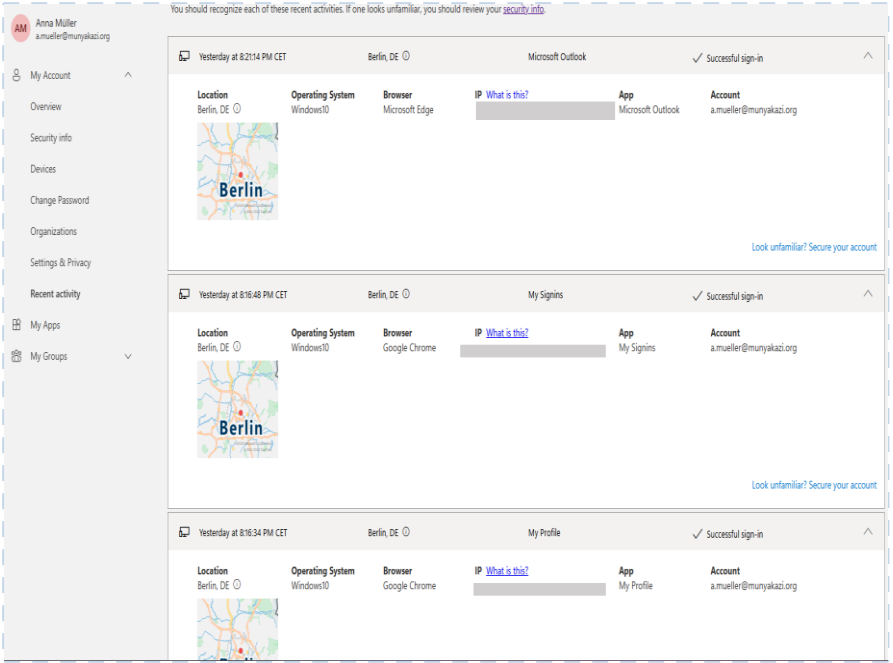
The first 30 minutes after a breach are the most critical. Quick action can:

- Prevent attackers from accessing more accounts
- Stop data from being stolen or encrypted
- Protect colleagues whose accounts may be targeted next

Delaying the report gives attackers more time. IT needs to act immediately; your speed matters.

STEP 1

Recognise the Warning Signs



INSTRUCTIONS

Signs that your account or device may be compromised:

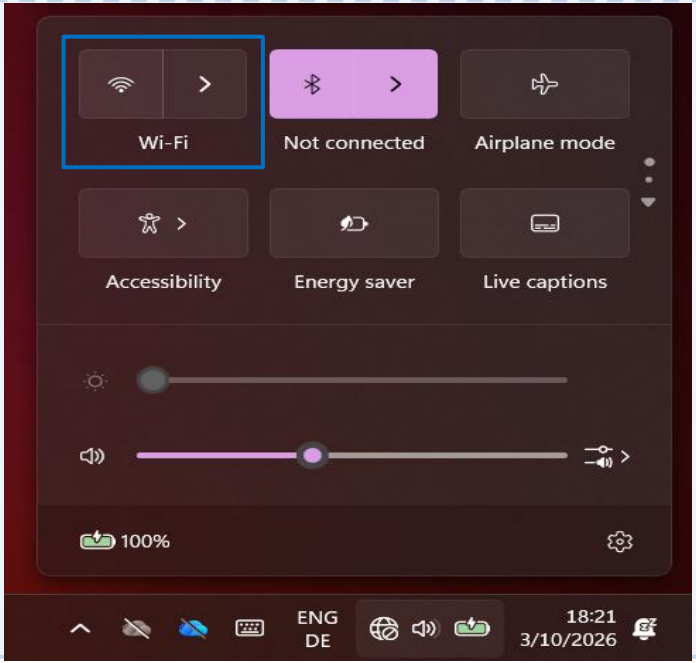
🚨 You receive a login alert for a location you don't recognise
🚨 Colleagues receive emails you didn't send
🚨 You are suddenly logged out of your accounts
🚨 Your password no longer works
🚨 Files appear encrypted or renamed strangely
🚨 Your computer is slow or acting unusually
🚨 Your browser opens unexpected websites

Go to myaccount.microsoft.com → Security → Sign-in activity

→ If you see ANY of these signs; stop what you are doing and go to Step 2

STEP 2

Immediate Actions — First 5 Minutes



INSTRUCTIONS

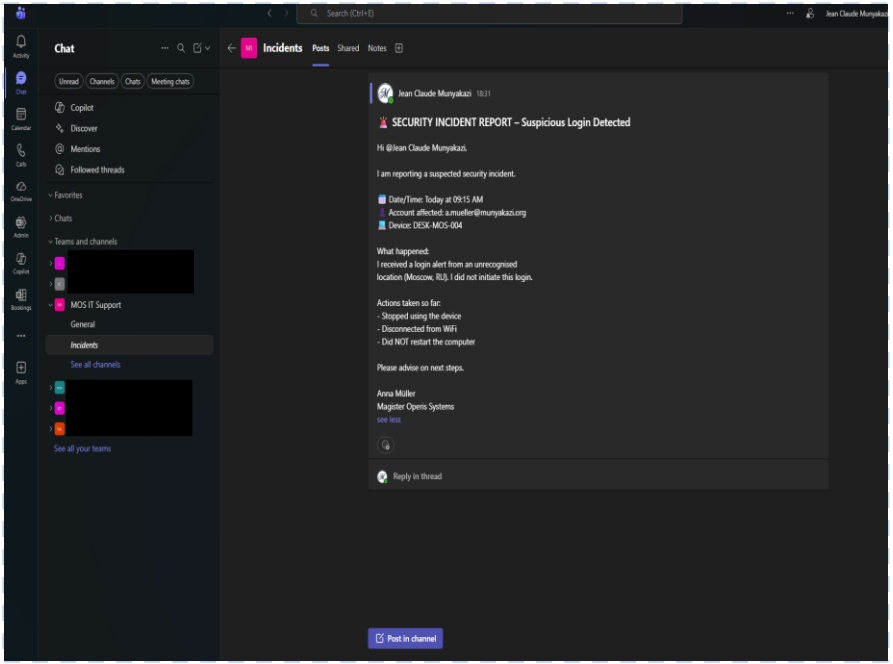
Do this immediately:

1. Stop using the affected device; do not close applications
2. Disconnect from the internet if possible:
   → Unplug network cable OR turn off WiFi
   → This stops attackers from accessing your device remotely
3. Do NOT turn off or restart your computer
   → Important evidence may be lost
4. Do NOT delete suspicious emails or files
5. Take a photo of your screen with your phone if there is anything unusual

→ Go immediately to Step 3

STEP 3

Contact IT Immediately



INSTRUCTIONS

Contact IT within 30 minutes of noticing the issue:

Option 1: Teams (from another device):
→ MOS IT Support channel → Post in Incidents tab
→ Tag: @Jean Claude Munyakazi

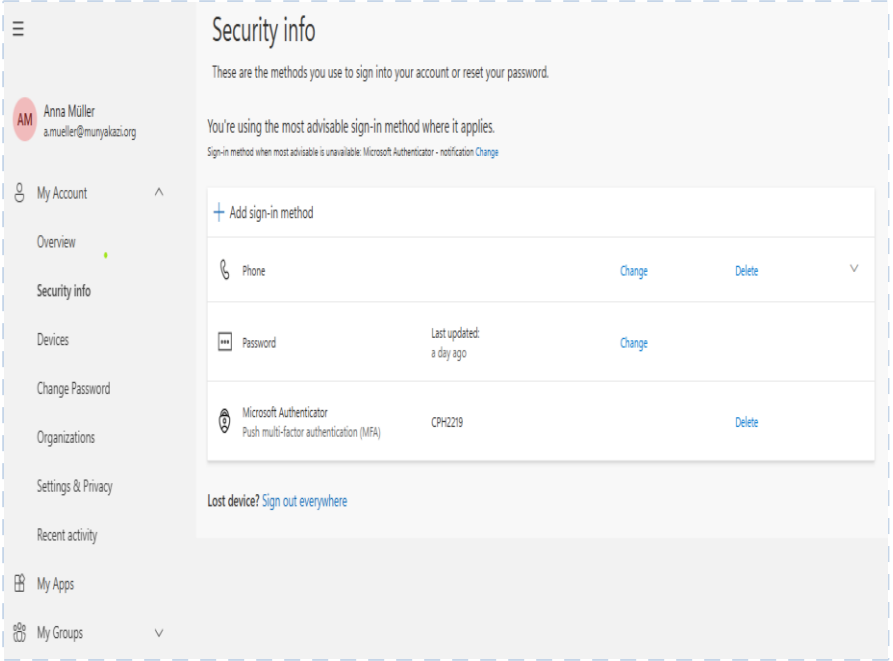
Option 2: Email (from personal email if company is affected):
→ itsupport@munyakazi.org

Option 3: In person:
→ Come directly to IT if the situation is urgent

Tell IT:
- What you noticed and when
- What you clicked or did before it happened
- Whether you see anything unusual on screen right now

STEP 4

After IT Responds — Change Your Credentials



INSTRUCTIONS

Once IT gives you the all-clear, change your credentials:

1. Change your Windows password (Ctrl + Alt + Delete → Change password)

2. Change your M365 password at: myaccount.microsoft.com

3. Review your Security info for any sign-in methods you don't recognise
   → Remove any unknown phone numbers or apps

4. Check: myaccount.microsoft.com → Recent activity
   → Look for logins from unfamiliar locations

5. Follow IT's instructions exactly; they may have additional steps

What NOT To Do

Don't try to fix it yourself first

Well-intentioned actions (restarting, deleting files, changing settings) can destroy forensic evidence IT needs.

Don't notify colleagues before notifying IT

Sharing unconfirmed information can cause panic. Let IT assess and communicate the situation officially.

Don't stay silent hoping it will resolve itself

Security incidents do not resolve themselves. Every minute of delay gives attackers more access.

Don't reuse old passwords when resetting

If your password was compromised, create a completely new strong password; not a variation of the old one.

Don't continue working on the affected device

Using a compromised device can spread the infection to more company systems and files.

Don't assume it was your fault

Sophisticated phishing attacks fool security experts. Report without fear; fast reporting is what matters.

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

What To Do If You're Hacked

1. Recognise warning signs: unexpected logins, locked accounts, strange emails
2. Stop using the device immediately; disconnect from internet, do NOT restart
3. Contact IT within 30 minutes: Teams → MOS IT Support → Incidents
4. Do not delete evidence; IT needs to investigate the device as-is
5. After IT confirms: change Windows and M365 passwords, review Security info
6. Report without fear; acting fast is what protects the company