🛡️ Cybersecurity Awareness Tips

Ministry of Finance – Staff Reference Sheet

> ***Note:*** *This is not an official publication of the Ministry of Finance but reflects standard cybersecurity best practices expected of all staff handling digital systems and sensitive data.*

🔐 *Stay Alert. Stay Secure.*

Cybersecurity is everyone's responsibility. Follow these key tips to protect Ministry data, systems, and your own digital safety:

✅ *Best Practices*

- ***Use Strong Passwords:***
  Combine upper/lowercase letters, numbers, and symbols. Avoid using your name or birthdate.

- ***Change Passwords Regularly:***
  Update passwords every 90 days or immediately after a suspected compromise.

- ***Enable Two-Factor Authentication (2FA):***
  Where available, always enable 2FA for added account protection.

- ***Lock Your Devices:***
  Use screen locks and always log off or lock your screen when stepping away.

- ***Be Email Smart:***
  Verify sender addresses. Hover over links before clicking. Never open unexpected attachments.

🚫 *Avoid These Mistakes*

- ***Don’t Share Passwords:***
  No one—not even IT—should ask for your password.

- ***Avoid Public Wi-Fi for Work:***
  Use only secure and trusted networks for ministry-related work.

- ***Don't Download from Unknown Sources:***
  All downloads must be from approved or official websites.

- ***No Personal Devices on Ministry Network:***
  Avoid connecting personal USBs, laptops, or phones unless cleared by IT.

⚠️ *Spot and Report Threats*

- ***Phishing Emails:*** *Look for urgent language, strange requests, or unfamiliar links.*

- ***Malware or Virus Signs:*** *Sluggish system performance, pop-ups, or unauthorized changes.*

- ***Suspicious Activity:*** *Report any strange login alerts, files, or software behavior.*

📞 *If in Doubt – Report Immediately*

IT Support Desk
📧*: support@mof.gov.gh* 📞*: Ext. 204 / 0800 900 104*
🕑 *Mon–Fri, 8:00 AM–5:00 PM*

Issued by the IT Department – Ministry of Finance | All Rights Reserved