



# IT Knowledge Sharing Session

# Things on my mind that I'd like to share



- Workspace Application
- Data Analysis Tools
- Data Storage and Security
- Dedicated Tools for NMC
- Use of artificial intelligence



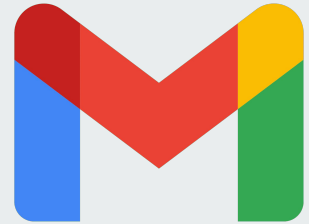
# Uses of Workspace Applications





# Gmail Address for NMC

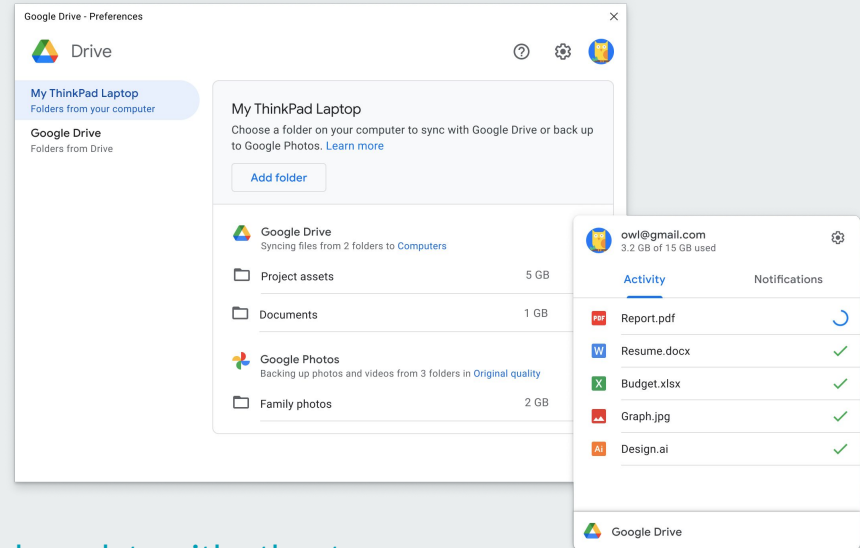
saklayen.nmc@gmail.com\*




\* Use a passkey instead of a password to log in to Gmail with two-factor or multi-factor authentication.

# Google Drive Desktop\*

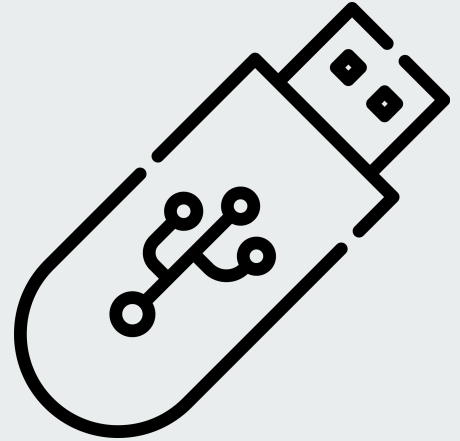
- Sync your PC with Google Drive
- Backup and access all of your content directly from PC



\* A centralized drive that all employees can access in order to share data with other teams.



**Don't try to use  
external drive**





# Google Meet

- Integrated with other google apps easily
- Set meeting with your team instantly





# Google Chat

- Multiple Communication Channels
- Screen Sharing
- Integration with Google Products
- Conduct Virtual Meetings



Chat





# Google Task

- Easy to create to-do lists.
- Create reminders and notifications.





# Google Keep

- Add others to the note to share and collaborate
- Set for reminders.





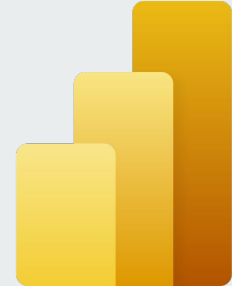
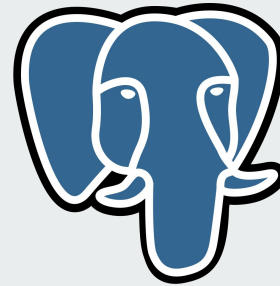
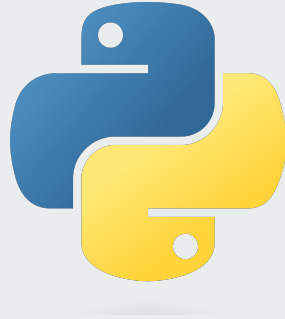
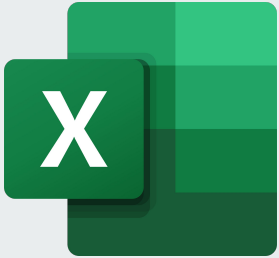
# IT systems for NMC\*

- Employee database management system
- Timesheet management system
- Asset allocation management System
- Appraisal management system



\* Coming soon.

# Data Analysis Tools



# Data Analysis Tools



Tableau Data Analysis Software



Microsoft Excel



Python Programming Language



R Programming Language



Google Sheet



Microsoft Power BI

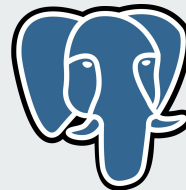
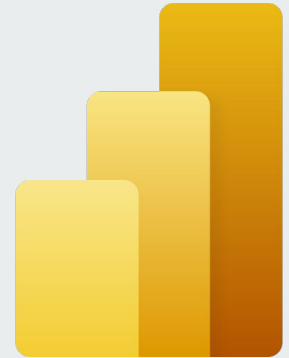


PostgreSQL, MySQL, Microsoft SQL Studio



PostgreSQL

# Data Analysis Tools for Us



PostgreSQL to enhance SQL Knowledge



# Use of Artificial Intelligence tools\*

- Bard - Google
- Bing Chat (GPT 4) - Microsoft
- ChatGPT (GPT 3.5) - OpenAI
- Grok - Xai (Elon Mask)

\* It may display inaccurate info, including about people and other information, so double-check its responses

**Q&A**



# **Interactive Q&A: Workplace Security**



## Scenario 01



You receive an email from an unknown sender with a subject line that says you've won a lottery you never entered. The email asks for your personal information to claim your prize. What should you do?

- A.** Reply with your personal information to claim the prize.
- B.** Ignore the email and delete it.
- C.** Forward the email to your friends for their opinion.
- D.** Investigate the email further and see if it's a genuine offer.

**Correct Answer: B. Ignore the email and delete it.**



**A. Reply with your personal information to claim the prize.**

**Explanation:** Never share personal information with unknown or unverified sources. This is a classic phishing attempt.

**B. Ignore the email and delete it.**

**Explanation:** This is the correct choice. If you receive unsolicited emails claiming you've won something, especially if you didn't enter a lottery, it's best to ignore and delete them.

**C. Forward the email to your friends for their opinion.**

**Explanation:** Forwarding such emails may potentially expose your friends to scams. It's better to avoid sharing suspicious messages.

**D. Investigate the email further and see if it's a genuine offer.**

**Explanation:** While being cautious is good, it's often best to err on the side of caution and delete unsolicited messages that seem too good to be true. Investigating further may involve unnecessary risks.

## Scenario 02



You receive an email that appears to be from a trusted colleague, asking you to download an attached document. However, the email looks suspicious, and the sender's email address is slightly different from the usual one. What should you do?

- A.** Download and open the attachment without hesitation.
- B.** Verify the sender's identity and the email's legitimacy before downloading.
- C.** Forward the email to your IT department for them to handle.
- D.** Send a reply asking the colleague for more information.

**Correct Answer: B. Verify the sender's identity and the email's legitimacy before downloading.**



**A. Download and open the attachment without hesitation.**

**Explanation:** This is risky behavior. If the email appears suspicious, downloading the attachment without verification can lead to malware infections.

**B. Verify the sender's identity and the email's legitimacy before downloading.**

**Explanation:** This is the correct choice. If an email seems suspicious or if the sender's address doesn't match the usual one, you should verify the sender's identity and the email's legitimacy before taking any action.

**C. Forward the email to your IT department for them to handle.**

**Explanation:** It's a good practice to involve your IT department if you suspect a suspicious email. However, the initial step should be personal verification before forwarding.

**D. Send a reply asking the colleague for more information.**

**Explanation:** While contacting the colleague for verification is a good step, it's important not to directly reply to the suspicious email. Instead, use known contact details to reach out and confirm the request.

### Scenario 03



You are browsing a website, and a pop-up message appears claiming that your computer is infected with a virus. It offers a phone number to call for immediate assistance. What should you do?

- A.** Call the provided phone number for help in removing the virus.
- B.** Click on the pop-up to initiate a virus scan.
- C.** Close the pop-up and continue browsing as usual.
- D.** Use your antivirus software to scan your computer for malware.

**Correct Answer: D. Use your antivirus software to scan your computer for malware.**



**A. Call the provided phone number for help in removing the virus.**

**Explanation:** You should never call the provided phone number in such a pop-up. This is a common tech support scam. Scammers often use scare tactics to trick users into paying for unnecessary services.

**B. Click on the pop-up to initiate a virus scan.**

**Explanation:** Clicking on the pop-up can lead to malware or further scams. Do not interact with these pop-ups; they are typically fraudulent.

**C. Close the pop-up and continue browsing as usual.**

**Explanation:** This is a reasonable action. Close the pop-up and ignore it. However, it's still advisable to use your antivirus software to scan your computer for any potential threats.

**D. Use your antivirus software to scan your computer for malware.**

**Explanation:** This is the correct choice. Always rely on your trusted antivirus software to perform security scans. If you encounter suspicious pop-ups, using your antivirus is a proactive and secure way to address potential threats.

## Scenario 04



You receive an email with a link that claims to be from a well-known online shopping site, offering a 90% discount on a popular item. The email looks convincing, but you're not sure if it's legitimate. What should you do?

- A.** Click the link to take advantage of the discount.
- B.** Forward the email to your friends to share the deal.
- C.** Go directly to the shopping site by typing the URL in your browser.
- D.** Click the link and proceed with the purchase.

**Correct Answer: C. Go directly to the shopping site by typing the URL in your browser.**



**A. Click the link to take advantage of the discount.**

**Explanation:** Clicking on links in unsolicited emails, especially those promising incredible deals, can lead to phishing sites or scams.

**B. Forward the email to your friends to share the deal.**

**Explanation:** Sharing such emails can potentially expose your friends to scams. It's best not to forward unsolicited emails.

**C. Go directly to the shopping site by typing the URL in your browser.**

**Explanation:** This is the correct choice. If you receive an unsolicited email with an offer, it's safest to go to the official website by typing its URL directly into your browser. This way, you avoid potential phishing scams.

**D. Click the link and proceed with the purchase.**

**Explanation:** Clicking on the link in an unsolicited email can be risky. It's always better to independently verify the offer's legitimacy by visiting the official website.



## Scenario 05



You're on a public Wi-Fi network, and you want to access your online banking account to check your balance. What should you do to secure your connection?

- A.** Access your online banking account without any extra precautions.
- B.** Use a Virtual Private Network (VPN) to encrypt your connection.
- C.** Disable your firewall to improve connection speed.
- D.** Use a simple, easy-to-guess password for your banking account.

**Correct Answer: B. Use a Virtual Private Network (VPN) to encrypt your connection.**



**A. Access your online banking account without any extra precautions.**

**Explanation:** Accessing sensitive accounts on public Wi-Fi without extra precautions can expose your data to potential eavesdropping. This is not secure.

**B. Use a Virtual Private Network (VPN) to encrypt your connection.**

**Explanation:** This is the correct choice. Using a VPN on public Wi-Fi encrypts your data, making it more secure and protecting your privacy.

**C. Disable your firewall to improve connection speed.**

**Explanation:** Disabling your firewall is not recommended, as it leaves your device vulnerable to security threats.

**D. Use a simple, easy-to-guess password for your banking account.**

**Explanation:** Using a simple password is never a good practice, especially for sensitive accounts. Strong, unique passwords are essential for online security.

## Scenario 06



You are using a cloud storage service to store important work-related documents. You receive an email with a link claiming to be from your cloud storage provider, asking you to verify your account details. What should you do?

- A.** Click the link and provide your account details to verify your account.
- B.** Ignore the email and continue using your cloud storage service as usual.
- C.** Forward the email to your colleagues for their opinion.
- D.** Contact your cloud storage provider through their official website or customer support.

**Correct Answer: D. Contact your cloud storage provider through their official website or customer support.**



**A. Click the link and provide your account details to verify your account.**

**Explanation:** This is a risky action. Clicking on links in unsolicited emails and providing account details can lead to phishing or compromise of your account.

**B. Ignore the email and continue using your cloud storage service as usual.**

**Explanation:** This is a reasonable choice. It's safer to ignore suspicious emails and not engage with them, especially if they request sensitive information.

**C. Forward the email to your colleagues for their opinion.**

**Explanation:** While it's good to seek opinions from colleagues, forwarding such emails can potentially expose others to phishing scams. The initial step should be personal verification.

**D. Contact your cloud storage provider through their official website or customer support.**

**Explanation:** This is the correct choice. To verify the legitimacy of the email, you should independently contact your cloud storage provider through their official channels, such as their website or customer support. Do not trust links in unsolicited emails.

## Scenario 07



You have sensitive personal documents stored in your online cloud storage account. You access your account using a weak and easily guessable password. What should you do to enhance the security of your online storage?

- A.** Continue using the weak password; it's convenient.
- B.** Use a strong, unique password for your online storage account.
- C.** Share your password with a trusted friend in case you forget it.
- D.** Set up two-factor authentication (2FA) for your online storage account.

**Correct Answer: D. Set up two-factor authentication (2FA) for your online storage account.**



**A. Continue using the weak password; it's convenient.**

**Explanation:** Using a weak password is not advisable, as it can make your account vulnerable to hacking.

**B. Use a strong, unique password for your online storage account.**

**Explanation:** This is a good practice. Using a strong and unique password enhances the security of your online storage account.

**C. Share your password with a trusted friend in case you forget it.**

**Explanation:** Sharing your password with anyone, even a trusted friend, is a security risk. It's not recommended.

**D. Set up two-factor authentication (2FA) for your online storage account.**

**Explanation:** This is the correct choice. Enabling two-factor authentication (2FA) adds an extra layer of security to your account. It requires a second authentication factor, making it more difficult for unauthorized users to access your account even if they have your password.

## Scenario 08



You're an employee in an office, and you need to transfer some sensitive work files to a colleague. You have the option to use a portable external drive or a secure cloud storage service. What potential security risks should you consider when deciding which method to use?

- A.** There are no security risks when using a portable drive; it's a safe and reliable option.
- B.** Using a portable drive can expose your data to malware if the drive is infected.
- C.** Cloud storage is always less secure than using a portable drive.
- D.** Portable drives are immune to data theft and unauthorized access.

**Correct Answer: B. Using a portable drive can expose your data to malware if the drive is infected.**



**A. There are no security risks when using a portable drive; it's a safe and reliable option.**

**Explanation:** This option is incorrect. Portable drives can pose security risks, including the potential for malware infection and data theft.

**B. Using a portable drive can expose your data to malware if the drive is infected.**

**Explanation:** This is the correct choice. Portable drives can carry malware from one computer to another if they are infected. This is a significant security risk.

**C. Cloud storage is always less secure than using a portable drive.**

**Explanation:** This is not accurate. Cloud storage can offer robust security measures and encryption, making it a secure option when used properly.

**D. Portable drives are immune to data theft and unauthorized access.**

**Explanation:** This option is incorrect. Portable drives can be lost or stolen, which could result in data theft and unauthorized access.



## Scenario 09



You have confidential work files stored on your office computer, and you need to access them from home. You're considering transferring the files to a portable drive to work from home. What is a more secure alternative to using a portable drive for remote access to your files?

- A. Using a password-protected portable drive to transfer the files.
- B. Emailing the files to your personal email account and downloading them at home.
- C. Uploading the files to a secure cloud storage service and accessing them remotely.
- D. Using a file-sharing service without encryption to transfer the files.

**Correct Answer: C. Uploading the files to a secure cloud storage service and accessing them remotely.**



**A. Using a password-protected portable drive to transfer the files.**

**Explanation:** While password protection is a good step, it's not as secure as using a cloud storage service with encryption and access controls.

**B. Emailing the files to your personal email account and downloading them at home.**

**Explanation:** Emailing sensitive files to a personal account is not secure and exposes the data to potential privacy and security risks.

**C. Uploading the files to a secure cloud storage service and accessing them remotely.**

**Explanation:** This is the correct choice. Using a secure cloud storage service and accessing files remotely is a more secure and convenient option. It offers encryption and access control, reducing security risks.

**D. Using a file-sharing service without encryption to transfer the files.**

**Explanation:** Using a file-sharing service without encryption is not a secure way to handle sensitive work files, as it can expose the data to potential data breaches.

## Scenario 10



Your company frequently conducts online meetings with external clients. How can you verify the authenticity of an external client's video conferencing link to avoid falling victim to phishing or impersonation attacks?

- A.** Click the link provided by the external client without any verification.
- B.** Verify the link's authenticity by contacting the external client directly.
- C.** Share the link with your colleagues for their opinion.
- D.** Request the external client to provide their email password for verification.

**Correct Answer: B. Verify the link's authenticity by contacting the external client directly.**



**A. Click the link provided by the external client without any verification.**

**Explanation:** Clicking on links without verification can be risky, as it could lead to phishing attacks.

**B. Verify the link's authenticity by contacting the external client directly.**

**Explanation:** This is the correct choice. To ensure the link is legitimate, contact the external client directly through trusted communication channels to verify the link.

**C. Share the link with your colleagues for their opinion.**

**Explanation:** Sharing the link with colleagues may not necessarily provide the security verification required.

**D. Request the external client to provide their email password for verification.**

**Explanation:** Requesting an email password is never a secure method for verification and should be avoided.

## Scenario 11



You're using an online chatting app for work-related communication with colleagues. You receive a message from a colleague containing a link to a file-sharing service. What security concerns should you consider before clicking on the link?

- A.** Click the link immediately; it's from a colleague, so it should be safe.
- B.** Verify the link's authenticity by contacting your colleague to confirm its legitimacy.
- C.** Share the link with other colleagues to see if they think it's safe.
- D.** Disable your antivirus software temporarily to access the file more quickly.

**Correct Answer: B. Verify the link's authenticity by contacting your colleague to confirm its legitimacy.**



**A. Click the link immediately; it's from a colleague, so it should be safe.**

**Explanation:** Clicking on links without verification can be risky, even if they are from colleagues. You should always exercise caution to prevent potential security risks such as phishing.

**B. Verify the link's authenticity by contacting your colleague to confirm its legitimacy.**

**Explanation:** This is the correct choice. Verifying the link with your colleague is a good practice to ensure that it's legitimate and not a potential security threat.

**C. Share the link with other colleagues to see if they think it's safe.**

**Explanation:** Sharing the link with other colleagues may not necessarily provide a reliable security verification. Relying on others' opinions may not be sufficient.

**D. Disable your antivirus software temporarily to access the file more quickly.**

**Explanation:** Disabling antivirus software is not a secure practice and should be avoided. It can expose your system to potential security threats.



# Questions?