**Programming 2A PROG6221**

**Dr.Mpho Gololo**

**POE**

**ST10259834**

Contents

[GitHub Repo Link 3](#_Toc201952938)

[Information used in chatbot 3](#_Toc201952939)

[References 6](#_Toc201952940)

# GitHub Repo Link

https://github.com/IIEWFL/prog6221-poe-ST10259834-Aaryan-Makan

# Information used in chatbot

**Password-Related Information**

* **Create strong passwords**: "🔐 Create strong passwords with at least 12 characters, including uppercase, lowercase, numbers, and symbols (e.g., P@ssw0rd!2025). Avoid common words or personal info like birthdays."
* **Avoid reusing passwords**: "🚫 Never reuse passwords across different websites or accounts. If one site is compromised, hackers can use the same password to access other accounts."
* **Enable two-factor authentication (2FA)**: "🔒 Enable two-factor authentication (2FA) whenever available. This adds a second verification step, like a code sent to your phone, making it harder for attackers to gain access."
* **Change passwords regularly**: "🔄 Change passwords every 6-12 months, or immediately if a service reports a data breach. Use a password manager like LastPass or Bitwarden to securely store and generate unique passwords."
* **Avoid sharing passwords insecurely**: "⚠️ Avoid sharing passwords via email, text, or unsecured apps. If you must share, use a secure method like an encrypted messaging app or a one-time password-sharing tool."
* **Quiz Question**: "Should you reuse passwords?" with options ["True", "False"], correct answer index 1 (False), and explanation "Using unique passwords reduces the risk of multiple accounts being compromised."
* **What should a strong password include?**: Question with options ["Letters and numbers", "Symbols", "All of the above"], correct answer index 2 (All of the above), and explanation "Strong passwords include a mix of letters, numbers, and special characters."
* **Supportive response**: "😟 I can sense you're worried. Cybersecurity can be daunting, but small steps make a big difference. For example, using strong passwords and enabling 2FA can protect your accounts. Try typing 'password' for tips or 'quiz' to test your knowledge!"

**Phishing-Related Information**

* **Verify sender’s email address**: "📧 Always verify the sender’s email address. Scammers often use slightly altered domains (e.g., [support@paypa1.com](mailto:support@paypa1.com) instead of [support@paypal.com](mailto:support@paypal.com)) to trick you into trusting fake messages."
* **Be cautious of unsolicited messages**: "🚨 Be cautious of unsolicited emails, texts, or calls with urgent demands, like 'Your account is locked!' These are common phishing tactics to steal your credentials or money."
* **Avoid clicking links or downloading attachments**: "🔍 Don’t click on links or download attachments from unknown sources. Hover over links to check the URL, and scan files with antivirus software before opening."
* **Use spam filters and report phishing**: "🛡️ Use spam filters in your email client and report suspicious messages as phishing. Services like Gmail and Outlook have built-in tools to flag and block scam attempts."
* **Stay informed about scams**: "🧠 Stay informed about common scams, like fake tech support calls, lottery frauds, or romance scams. If an offer seems too good to be true, it probably is—verify before acting."
* **Quiz Question**: "How do you spot a phishing scam?" with options ["Grammar mistakes", "Urgency", "All of the above"], correct answer index 2 (All of the above), and explanation "Phishing scams often use urgency and errors to trick users."
* **What should you do if you receive an email asking for your password?**: Question with options ["Reply with your password", "Delete the email", "Report the email as phishing", "Ignore it"], correct answer index 2 (Report the email as phishing), and explanation "Reporting phishing emails helps prevent scams."
* **Supportive response for frustration**: "😣 Frustration is understandable—cyber threats are tricky! Let’s simplify things. You can learn about avoiding scams or securing your browsing. Type 'scam' or 'privacy' for detailed advice, or use the right panel to manage tasks and stay organized."
* **Encouraging curiosity**: "🤔 Curiosity is a great start! Cybersecurity is all about staying one step ahead. Explore topics like phishing scams or VPNs by typing 'scam' or 'privacy', or try the quiz to dive deeper into key concepts!"
* **Topic selection**: Option "2" or "phishing scams" triggers the "scam" keyword responses.

**Privacy-Related Information**

* **Use a VPN on public Wi-Fi**: "🌐 Use a Virtual Private Network (VPN) on public Wi-Fi to encrypt your data. Free Wi-Fi at cafes or airports can be targeted by hackers to intercept sensitive information."
* **Review social media privacy settings**: "🔐 Regularly review privacy settings on social media platforms like X or Facebook. Limit who can see your posts, avoid sharing sensitive details like your address, and disable location tagging."
* **Block unnecessary app permissions**: "🚫 Block unnecessary app permissions on your phone or computer. For example, a flashlight app doesn’t need access to your contacts or location—check and revoke permissions in settings."
* **Clear browser cookies and cache**: "🗑️ Clear browser cookies and cache monthly to reduce tracking by advertisers and websites. Use browsers like Firefox with enhanced tracking protection for better privacy."
* **Avoid oversharing online**: "🔍 Be mindful of oversharing online. Avoid posting sensitive information like travel plans or financial details, as scammers can use this to target you or impersonate you."
* **Quiz Question**: "Is public Wi-Fi safe for online banking?" with options ["True", "False"], correct answer index 1 (False), and explanation "Public Wi-Fi can be insecure; use a VPN for sensitive activities."
* **What is a VPN used for?**: Question with options ["Encrypt traffic", "Speed up internet"], correct answer index 0 (Encrypt traffic), and explanation "A VPN encrypts your internet traffic for security."
* **Topic selection**: Option "3" or "safe browsing" triggers the "privacy" keyword responses.

**General Cybersecurity and Quiz-Related Information**

* **What does HTTPS stand for?**: Question with options ["HyperText Transfer Protocol Secure", "Hyper Terminal Secure", "Host Transfer Secure"], correct answer index 0, and explanation "HTTPS indicates a secure, encrypted connection."
* **What is two-factor authentication?**: Question with options ["Two-Factor Authentication", "Two-Faced Algorithm", "Too Fast Access"], correct answer index 0, and explanation "Two-factor authentication adds an extra layer of security."
* **Are browser updates important?**: Question with options ["True", "False"], correct answer index 0 (True), and explanation "Browser updates fix security vulnerabilities."
* **Social engineering definition**: Question "Social engineering involves manipulating people to gain confidential information." with options ["True", "False"], correct answer index 0 (True), and explanation "Social engineering exploits human psychology to bypass security."
* **Quiz initiation**: "Initiates a 10-question cybersecurity quiz to test user knowledge." with options to start via "quiz" command or "Start Quiz" button.
* **Quiz feedback**: Score-based feedback ("🏆 Great job! You're a cybersecurity pro!" for ≥8, "📘 Good effort! Keep learning to stay safe online!" for ≥5, "📚 You might want to review cybersecurity basics!" for <5).

**User Interaction and Supportive Responses**

* **Worried user support**: "😟 I can sense you're worried. Cybersecurity can be daunting, but small steps make a big difference. For example, using strong passwords and enabling 2FA can protect your accounts. Try typing 'password' for tips or 'quiz' to test your knowledge!"
* **Frustrated user support**: "😣 Frustration is understandable—cyber threats are tricky! Let’s simplify things. You can learn about avoiding scams or securing your browsing. Type 'scam' or 'privacy' for detailed advice, or use the right panel to manage tasks and stay organized."
* **Curious user encouragement**: "🤔 Curiosity is a great start! Cybersecurity is all about staying one step ahead. Explore topics like phishing scams or VPNs by typing 'scam' or 'privacy', or try the quiz to dive deeper into key concepts!"
* **Topic options**: "Select a topic to begin learning: 1. Password Safety\n2. Phishing Scams\n3. Safe Browsing Tips" with guide for further interaction.

# 

# References

**Norton (2023)** *What is phishing? How to spot and avoid it*. [online] Available at: <https://us.norton.com/blog/online-scams/what-is-phishing> (Accessed 27 June 2025).  
– Explains phishing as a form of social engineering and provides tips to recognize and avoid phishing scams [support.google.com+10us.norton.com+10us.norton.com+10](https://us.norton.com/blog/online-scams/what-is-phishing?utm_source=chatgpt.com).

**Kaspersky (2025)** *How to create a strong password and remember it*. [online] Available at: <https://www.kaspersky.com/resource-center/threats/how-to-create-a-strong-password> (Accessed 27 June 2025).  
– Covers guidelines for creating long, complex, and memorable passwords [kaspersky.com](https://www.kaspersky.com/resource-center/threats/how-to-create-a-strong-password?utm_source=chatgpt.com)[lastpass.com+2blog.lastpass.com+2blog.lastpass.com+2](https://blog.lastpass.com/posts/how-to-train-employees-on-secure-password-practices?utm_source=chatgpt.com).

**LastPass (2024)** *Password 101: Password basics to keep you safe*. [online] Available at: <https://www.lastpass.com/resources/learning/password-101> (Accessed 27 June 2025).  
– Summarizes best practices: unique, complex passwords, frequent changes, and avoiding reuse [lastpass.com](https://www.lastpass.com/resources/learning/password-101?utm_source=chatgpt.com).

**Google (2025)** *Tips to stay safe & secure online* – Safety Center. [online] Available at: <https://www.google.com/safetycenter/everyone/start/devices/> (Accessed 27 June 2025).  
– Offers advice on strong/unique passwords and recognizing phishing attempts [google.com+1privacy.google.com+1](https://www.google.com/safetycenter/everyone/start/devices/?utm_source=chatgpt.com).

**Microsoft (2025)** *What Is Two‑Factor Authentication (2FA)?* [online] Available at: <https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa> (Accessed 27 June 2025).  
– Defines 2FA/2-step verification and explains how it strengthens account security