

Session 2: Keeping Your Accounts Safe

Many things we do online depend on accounts and logins. If someone gets into your account, they can see your messages, use your name, or misuse your information. This session is about passwords, OTPs, privacy settings, and fake messages.

Session Objective

By the end of this session, you will be able to:

- Understand what makes a strong password.
- Keep OTPs and login details private.
- Use basic privacy settings.
- Spot suspicious messages, links, and login requests.
- Know what to do when something feels fake or urgent.

Account safety habits

Habit	Action/Description
Use Strong Passwords	Create unique, complex passwords using letters, numbers, and symbols.
Keep Credentials Private	Never share OTPs, PINs, or login details with anyone.
Maintain Privacy	Regularly review and use privacy settings on all your apps.
Secure Sessions	Always log out of accounts when using public or shared devices.

Habit	Action/Description
Keep Software Updated	Ensure apps and operating systems are updated to the latest versions.

What is a strong password?

A strong password is not your name, birthday, or phone number. It is not "1234" or "password". It uses a mix of letters, numbers, and symbols, and is different from the password you use for other accounts.

What should stay private online?

Private Information	Reason for Privacy
Passwords	Must remain confidential to prevent unauthorized access.
OTPs	Must remain confidential to prevent unauthorized access.
PINs	Must remain confidential to prevent unauthorized access.
Security Answers	Must remain confidential to prevent unauthorized access.
Recovery Codes	Must remain confidential to prevent unauthorized access.
Net Banking Details	Must remain confidential to prevent unauthorized access.
ATM PINs	Must remain confidential to prevent unauthorized access.

Messages that should make you pause

Suspicious Message	Why It's a Warning Sign
--------------------	-------------------------

"Your account will be blocked if you do not click now."	Creates false urgency to panic you.
"You have won a prize. Click to claim."	Too good to be true; often leads to scams.
"Send your OTP to verify."	Legitimate services will never ask for your OTP.
"Install this app urgently."	Often a trick to install malicious software.

Story: Sneha and the urgent message

Sneha is 17. She receives a message that looks like it is from a popular app. It says her account will be suspended unless she clicks a link and confirms her OTP. Sneha feels nervous. The message looks urgent. She notices a small spelling mistake and a strange link. She decides not to click and shows it to a staff member. The staff member tells her it is fake and asks her to delete and block.

Activity 1: True or False

- It is okay to share your OTP with a friend.
☐ True ☐ False
- A strong password should be easy to guess.
☐ True ☐ False
- You should use the same simple password everywhere.
☐ True ☐ False
- Privacy settings can help control who sees your posts.
☐ True ☐ False
- A message asking for your OTP should be checked carefully.
☐ True ☐ False

Activity 2: Safe or unsafe

6. Using a password like your name and birth year.
☐ Safe ☐ Unsafe
 7. Turning on privacy settings in an app.
☐ Safe ☐ Unsafe
 8. Sharing your login with a friend.
☐ Safe ☐ Unsafe
 9. Clicking on a message that says "claim now".
☐ Safe ☐ Unsafe
 10. Logging out after using a shared device.
☐ Safe ☐ Unsafe
 11. Keeping your software updated.
☐ Safe ☐ Unsafe
-

Activity 3: Spot the fake message

1. "Click this link to get a free prize."
☐ Safe ☐ Suspicious
 2. "Please send your OTP to verify your account."
☐ Safe ☐ Suspicious
 3. "Your friend tagged you in a photo."
☐ Safe ☐ Suspicious
 4. "Install this app now or your account will be blocked."
☐ Safe ☐ Suspicious
 5. "Check the sender and ask before replying."
☐ Safe ☐ Suspicious
-

Activity 4: Build a better password

Weak Password (Avoid)	Better Password (Example)
1234	Riya@4821
password	Sun#2026
anjali	M@ngo57!
111111	Blue@19Star

My own password pattern could be: _____

One thing I should avoid in my password is: _____

Activity 5: Fill in the blanks

1. Never share your _____ with anyone.
 2. A strong password should be hard to _____.
 3. OTP means one-time _____.
 4. Privacy settings help control who can see your _____.
 5. If a message feels urgent and strange, first _____ before acting.
-

Activity 6: What would you do?

1. What would you do if someone asked for your OTP? _____
 2. What would you do if a link looks suspicious? _____
 3. Why is it useful to keep your account private? _____
 4. Who can you ask if you are not sure about a message? _____
-
-

Quick Recap

Topic	Key Takeaway
Password Safety	Passwords should be strong and private.
OTP Security	OTPs should never be shared.
Account Protection	Use privacy settings and keep software updated.
Threat Awareness	Fake messages often create urgency.
Seeking Support	If something feels wrong, stop and check with a trusted adult.

One line to remember

Private means private. Passwords, OTPs, and login details stay with me.

Revision #1

Created 2026-08-11 09:03:35 UTC by Yeshwanth

Updated 2026-08-11 09:04:28 UTC by Yeshwanth