PROTECTING YOURSELF

The presentation today focused on the various types of online scams, their aims, and how to protect oneself from them. It covered topics such as social engineering, identity theft, and the increasing risks posed by AI in scams. The presentation also provided practical steps to identify and avoid scams, manage fake accounts, and protect personal information.

1 AVOID LINKING YOUR SOCIAL MEDIA ACCOUNTS

Remove other account names from your profile bio.
Sign in to each account using different details such as unique passwords.

2 CREATE STRONG PASSWORDS:

Use a password generator to create strong, unique passwords.

Regularly update passwords and avoid using the same password for multiple accounts

3 ENABLE TWO-FACTOR AUTHENTICATION:

Set up two-factor authentication on all accounts to add an extra layer of security

4 PROTECT PERSONAL INFORMATION:

Keep personal information up to date and secure.

Avoid sharing sensitive information like phone numbers and birth dates on public profiles

5 MONITOR SOCIAL MEDIA ACCOUNTS:

Regularly check for signs of hacked or fake accounts.

Report and manage fake accounts promptly

6 USE REPUTABLE SITES FOR PURCHASES:

Verify the authenticity of websites before making purchases.
Use trusted payment systems and avoid moving away from them

7 STAY INFORMED ABOUT AI RISKS:

Be aware of how AI can be used in scams, such as sextortion.
You can't always detect AI-generated images and videos

8 SEEK HELP WHEN NEEDED:

Do not pay scammers; instead, collect evidence and report the scam.
Take all available security options to protect yourself from further damage

eyes open
SOCIAL MEDIA SAFETY