Module 2:
Data Privacy and Security

Developed by: Women in Data Steering Committee
under Women Entrepreneurship Data (WEData) Nepal project.

What is data?

- Values, facts that convey information about something.
- Wide variety of data and information is stored, generated, used, shared, accessed over the internet.
- Personal data - information that relates to an identified or identifiable individual when easily accessible may be misused, used without permission.
  - person's name, address, email address, phone number, social security number, date of birth, and other identifying information
  - sensitive information such as a person's race or ethnicity, political opinions, religious beliefs, health information, financial information, and criminal record

Activity 2.1

What can you find about me?

Search about us!

- Can we find out personal information, preference, etc.
- How may it be used for/ against us.

Your Data on Internet

- We create digital data and leave trail over the internet using different apps
- **Data breaches** have occurred on the past.
  - Facebook, Yahoo
  - Banks and Internet Service Providers

What to share/not share on social media platforms?

How to protect your data and be secure on internet?

- Don’t share data on internet/applications without being sure about the privacy and data policies.
  - Apps data settings
  - Terms and conditions

- Only install use trusted sites and apps
    - Google Play Store
    - Apple Apps Store

- Use antivirus softwares
- Use safe browser (https:)
- Use strong credentials, 2FA, never reuse passwords

Data Privacy

- Protection of an individual's personal information from being collected, used, or shared **without their knowledge or consent**
- Data privacy protects misuse of personal data that may be used for malicious intents like identity theft, fraud, or harassment.
- It also ensures individuals rights over their own data on how they are used, stored and confidentiality.

Data Security

- Data Security is measures taken to ensure data privacy so data are protected from unauthorized access, use or disclosure
- For digital data security it usually requires the technical measures like encryption and access controls.
- It ensures organization individuals sensitive data are protected from data breaches and cyber attacks.

How is your data used?

- Personal data is valuable commodity that is collected, analysed and used for variety of purpose
- **Targeted advertisement**
- **Recommendations**
- **Healthcare management**
- **National policy and security**

“If you are not paying for it, you are the product.”

Why is privacy and security necessary?

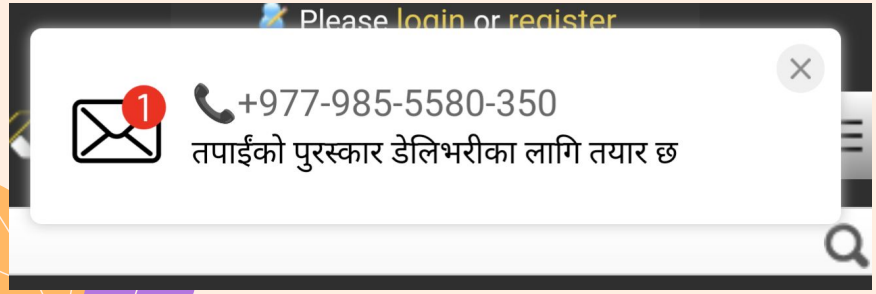
To minimize threats

- identity theft,
- reputational damage,
- financial losses,
- national security risks
- business disruptions


PC may be at risk
PC may be infected by viruses!
Google Chrome
Your antivirus may have expire
Renew NOW to stay protected
nokfr.ysearchingfo.xyz
Open
Remove Ads


Warning:
Your protection from viruses has expired!
Purchase a subscription now to fight back against malware and other cyber threats.
McAfee
Accept risk
Get protection


WARNING!
Your Computer May be Infected:
1 -5505
For emergency Tech Support call immediately
The system may have found (2) viruses that pose a serious threat
Browser.Hijacker.Spy ./ Trojan.FakeAV-Download
Your personal and financial information
may not be secured.
Call now for support
1 -5505


Please login or register
+977-985-5580-350
तपाईंको पुरस्कार डेलिभरीका लागि तयार छ

Threats to Data Privacy and Security

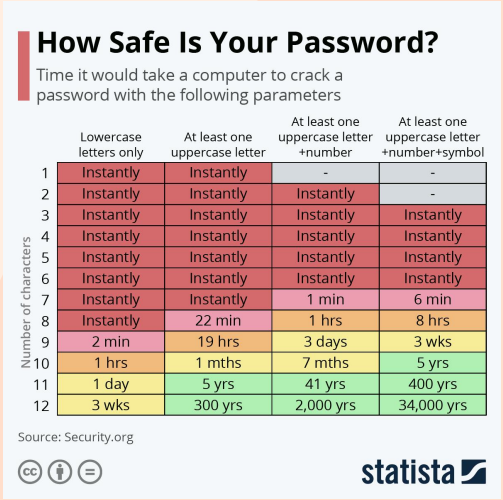
- Cyberattacks
- Malware
- Phishing Attacks
- Insider threats
- physical theft or loss
- social engineering
- data breaches

Threats to Data Privacy and Security

- Joint effort from service providers and users to stay safe from such threats
- Use anti-malware, ad blocker
- Regular updates of apps
- Use strong password
- Use encrypted communication services

Is your password Safe and Strong?

- Short and easy password may be easily cracked by guessing and using softwares.
  - names
  - phone numbers
  - birth years
- Recipe:
  - At least 8 characters
  - mix of lower case, upper case, and number
  - special characters



How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

statista

How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

statista

Password and 2 factor authentication

1 Factor - Strong and unique password to open the app
2 Factor - Text to smartphone or biometrics fingerprint, face, or retina to use app feature

It is not totally foolproof but provide better security to traditional methods

Activity 2.2

- Participants add 2-factor authentications to their social media profile or the gmail platform

- Try to use wrong authentication in second factor intentionally and simulate the environment where their password is breached

Allow 2-Step Verification

- Open your Google Account.
- In the navigation panel, select Security.
- Under “Signing in to Google,” select 2-Step Verification and then Get started
- Follow steps

Safe Internet

- Cyber Harassments
  - threat via the use of digital technologies
  - repeated behavior, aimed at threatening, scaring, shaming, and silencing targeted
  - Can take place on social media, messaging platforms, cell phones
- Cyber Laws
  - Electronic Transactions Act 2063
  - Privacy Act 2018
  - Information Technology Bill 2018

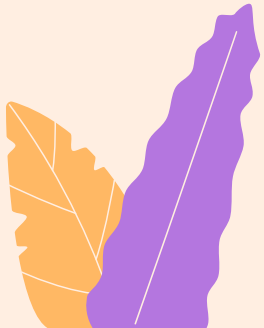
General tips for cyber security

- Think twice before posting or sharing anything online.
- Limit information you post on your account, especially personal details such as your address, telephone number, the name of your city/location, names of your relatives.
- Consider using communication application providing better privacy
- Only accept on personal social networks people you know.
- Warn your friends and acquaintances, not to post personal information about you.
- Don’t post photographs of your home that might indicate its location.

General tips for cyber security

- Learn about the privacy settings of your social media apps, including who can see your info and blocking/hiding contents options.
- Deactivate geo-location on all your accounts.
- Systematically check the background of your videos/Photos before publishing them.
- Report suspicious or threatening accounts.
- Keep private and business accounts strictly separate.
- Collect evidence

Any Question?



Thank You!!