ANDIJAN STATE PEDAGOGICAL INSTITUTE

Lecture materials · 2026–2027 academic year

SUBJECT

Information Systems and Digital Technologies

Lecture 15 · Data Security

2 hours

Lecturer: **Ismailov Alisher**

E-mail: alisherismailov1991@gmail.com

Contact: **99-499-73-64**

LECTURE 15 · 2 HOURS

FUNDAMENTALS OF COMPUTERS · TOPIC 9

Data Security

Keeping information safe: threats, encryption, passwords, backups and locks

CIA · AES · 2FA · 3-2-1



Four shields for your data

Your phone is lost on the bus. Now what?

What could a stranger see on your phone — and what would you lose for ever?

There are no wrong answers yet. We will return to this at the end of the lesson.



Think – Pair – Share (3 min)

1 Which data on your phone is the most private?

2 What protects it right now?

3 What would you do in the first ten minutes?

By the end of this lesson, you can…

1. **Explain** what data security is, using confidentiality, integrity and availability.
2. **Identify** threats to data: malware, phishing, hacking, human error and disasters.
3. **Describe** how encryption protects data, with symmetric and public-key examples.
4. **Create** strong passwords and use two-factor authentication and password managers.
5. **Plan** backups with the 3-2-1 rule and the steps of data recovery.
6. **Apply** physical security measures to devices, rooms and old storage media.

The CIA triad: three goals of data security

Data security = protecting digital information from unauthorised access, change or loss — for its whole life.

Confidentiality

Only authorised people can see the data. Example: only you and your teacher see your marks.

Integrity

Data stays correct and complete; nobody changes it without permission. Example: a mark cannot be secretly edited.

Availability

Data is there when it is needed. Example: the e-journal works on exam day.

Remember: every security measure protects at least one of C, I or A.

What are we protecting?

Personal data

Name, passport number, address, phone number, photos.

Financial data

Bank card numbers, payment apps, salary details.

Health records

Diagnoses, test results, prescriptions.

School and work records

Marks, exam papers, reports, contracts.

Ideas and creative work

Projects, designs, program code, research.

Login details

Usernames, passwords and one-time codes — the keys to everything else.

Threats to data security

Malware

Viruses, worms, trojans and spyware that damage or steal data.

Ransomware

Locks your files and demands money to unlock them.

Phishing

Fake messages that trick you into giving passwords or money.

Hacking

Breaking into systems without permission.

Weak passwords

Easy to guess, reused or leaked passwords.

Human error

Deleting files, sending data to the wrong person.

Disasters and failures

Fire, flood, power cuts and broken hard disks.

Theft and loss

Stolen or lost phones, laptops and USB sticks.

Malware: six kinds of harmful software

TYPE	How it works	A warning sign
Virus	Attaches to a file; spreads when the file is opened	Files change or will not open
Worm	Copies itself across a network with no help	The network suddenly becomes slow
Trojan horse	Pretends to be a useful program	A “free” app from an unknown site
Spyware	Secretly watches you and steals information	Accounts used without you
Ransomware	Encrypts your files and demands payment	A message asking for money
Adware	Floods the screen with unwanted adverts	Pop-ups everywhere

Defence: antivirus, updates, and installing apps only from official stores.

CHECK FOR UNDERSTANDING

Name that threat

A	A free game from an unknown website secretly sends your contacts to a stranger.
B	All files on the school computer are locked, with a message: “Pay to unlock”.
C	A student deletes the only copy of the class project by mistake.
D	An SMS asks you to “confirm your card” on a strange website.
E	A laptop is left on a café table and disappears.
F	A program spreads by itself to every computer in the lab.

Choose from

- Trojan / spyware
- Ransomware
- Human error
- Phishing
- Theft and loss
- Worm

Encryption: scrambling data with a key



Symmetric encryption

One shared secret key locks and unlocks.

Fast; used for files and disks. Example: AES.

Public-key encryption

A public key locks; only the private key unlocks.

Used for HTTPS and secure email. Example: RSA.

Try it: the Caesar cipher

How it works

shift every letter 3 places

- A → D B → E C → F … X → A
- DATA → GDWD
- The key is the number 3.
- Julius Caesar used it about 2 000 years ago.

Your challenge

shift back 3 places to decrypt

- Decrypt: VHFXUH
- Decrypt: KHOOR
- Encrypt your first name.
- Why is this cipher easy to break?

Today: real ciphers such as AES use keys so long that guessing them would take billions of years.

Encryption around you

HTTPS websites

The padlock in the address bar: data between you and the site is encrypted.

Secure messaging

End-to-end encryption: only sender and receiver can read.

Device encryption

Phones and laptops (e.g. BitLocker) encrypt the whole disk.

Wi-Fi security

WPA2 / WPA3 encrypt the radio signal of your network.

Key idea: a stolen laptop with an encrypted disk gives the thief a machine — but not your data.

CHECK FOR UNDERSTANDING

Encryption check

01 What is ciphertext?

02 Which kind of encryption uses one shared secret key?

03 Decrypt with a Caesar shift of 3: FRGH

04 What does the padlock next to a web address tell you?

05 Why is an encrypted laptop safer if it is stolen?

06 Public key or private key — which one must you keep secret?

What makes a password strong?

01

Long

12 or more characters. A passphrase of 4 random words is long and easy to remember.

02

Mixed

Upper and lower case, numbers and symbols.

03

Unique

A different password for every account.

04

Unpredictable

No names, birthdays, 123456, qwerty or “password”.

05

Secret

Never shared, never on a sticky note on the monitor.

06

Changed when leaked

Change it at once if a site reports a data leak.

How long would it take to guess?

PASSWORD	Why	Rough time to guess
123456	It is on every list of common passwords	Instantly
aziza2008	A name plus a year is a known pattern	Seconds to minutes
Tashkent2024!	Longer, but still a word, a year and a symbol	Hours to days
blue-river-samarkand-72	Long, random words — no pattern	Centuries

Note: rough estimates for guessing by a fast computer; real times vary.

Beyond passwords: 2FA and password managers

Two-factor authentication

two different proofs that it is you

- Something you KNOW: a password or PIN
- Something you HAVE: a phone code or security key
- Something you ARE: a fingerprint or face
- A stolen password alone is no longer enough.

Password managers

one strong vault for all your passwords

- Stores every password, encrypted
- Creates long random passwords for you
- You remember only one master password
- Examples: Bitwarden, and the managers built into phones and browsers

Golden rule: never tell anyone a one-time code — not even “the bank”.

CHECK FOR UNDERSTANDING

Strong or weak?

A	The password qwerty123
B	The password Barsik
C	The passphrase cloud-apricot-river-7
D	Using the same password for email and games
E	Turning on 2FA for your email
F	A sticky note with the password on the monitor

Write S or W

S = strong / safe habit

W = weak / risky habit

Bonus: fix every weak one.

Three types of backup

TYPE	What is copied	Speed and space	To restore you need
Full	Everything, every time	Slowest, most space	Only the last full backup
Incremental	Only what changed since the last backup of any kind	Fastest, least space	Full backup + every incremental since
Differential	Everything that changed since the last full backup	In between	Full backup + the last differential

Backup = an extra copy of data, kept separately, so it can be restored after loss.

The 3-2-1 backup rule

01

3 copies

The original and two backups.

02

2 different media

For example, the laptop’s SSD and an external disk.

03

1 copy off-site

In the cloud or in another building — safe from fire and theft.

And test it: a backup you have never restored is only a hope. Try restoring one file every month.

Data recovery: getting it back



Quick rescues

Recycle Bin / Trash

Version history in Google Docs and OneDrive

“Undo” straight after a mistake

When there is no backup

File-recovery software may find deleted files

Broken disks need a professional lab — slow and expensive

CHECK FOR UNDERSTANDING

Backup detective

01 Ransomware locks all your files. What saves you?

02 Which backup type is the fastest to make every day?

03 How many copies does the 3-2-1 rule ask for?

04 Is a USB stick kept in the same bag as the laptop an off-site backup?

05 You deleted a paragraph in a Google Doc yesterday. How do you get it back?

06 Why should you stop using a disk after deleting files by mistake?

Physical security: protecting the hardware

Locks and access cards

Server rooms and labs open only for authorised people.

Cameras and guards

CCTV and staff watch who comes in and out.

Screen lock

Lock the screen when you leave: Windows key + L.

Keep devices with you

Never leave phones or laptops unattended; use cable locks.

Power and fire protection

UPS, surge protectors, smoke detectors, fire extinguishers.

Safe disposal

Wipe or destroy old disks; shred paper with personal data.

Ten-second habits that protect your data

✓ DO

- Install updates as soon as they arrive
- Lock your screen every time you stand up
- Turn on 2FA for email and banking
- Back up automatically, and test it

✗ DON’T

- Click links in unexpected messages
- Plug in USB sticks you found or were given
- Install “cracked” programs from unknown sites
- Share passwords or one-time codes

CHECK FOR UNDERSTANDING

Which protection fits?

A	A thief steals a laptop, but cannot read any of its files.
B	A leaked password alone is not enough to open your email.
C	After a hard-disk crash, the school restores all marks by lunchtime.
D	Only staff with a key card can enter the server room.
E	A power cut happens, but the server shuts down safely.
F	An old hard disk is wiped with special software before it is sold.

Choose from

- Encryption
- Two-factor authentication
- Backup and recovery
- Access control
- UPS
- Secure disposal

Data security around you

BANKING

Paying with Click or Payme

→ SMS codes (2FA) + encryption

GOVERNMENT

Logging in to my.gov.uz with OneID

→ Identity checks + access control

SCHOOL

The e-journal keeps every mark

→ Passwords + daily backups

HOSPITAL

Patient records on a network

→ Access rights + encryption

BUSINESS

A company hit by ransomware

→ Offline backups save the day

YOU

Your phone

→ Screen lock + encryption + cloud backup

Review: can you answer these?

01 What do the letters C, I and A stand for?

02 Name four threats to data security.

03 How is a worm different from a virus?

04 What are plaintext, ciphertext and a key?

05 Give three rules for a strong password.

06 How does 2FA protect an account?

07 Explain the 3-2-1 backup rule.

08 Name three physical security measures.

Exit ticket

Answer on a slip of paper before you leave.

1. Name two threats to your data — one caused by people and one caused by accidents or nature.

2. Turn the weak password “samarkand” into a strong one, and explain what you changed.

3. Your laptop holds your final project. Write a backup plan that follows the 3-2-1 rule.