

Staying Safe Online

Identity, privacy, AI fakes and being a responsible digital citizen

THE QUESTION THIS UNIT ANSWERS

“What am I giving away, and how do I stay safe?”

SIX BIG IDEAS

- 1 Context is what makes data personal. The same fact can be harmless in one place and revealing in another.
- 2 Your footprint is what you post *and* what is collected about you. Deleting is not the same as removing.
- 3 Length beats complexity. Three unrelated words are stronger than one clever word.
- 4 Check the source, not the pixels. AI giveaways are disappearing; asking who posted it still works.
- 5 When something goes wrong: screenshot, block, report, tell. Being an upstander beats being a bystander.
- 6 Someone you met online is still a stranger, however long you have played together.

TWO HALVES OF ONE FOOTPRINT

ACTIVE	PASSIVE
What you choose to put there	What is collected anyway
Posts and photos	Cookies and trackers
Comments and replies	Location and device
Username and bio	What you watched
Sign-up forms	Screenshots by others

One record, and it lasts
The “future you” test: would you be happy for this to be found in ten years?

KEY VOCABULARY

Identity & personal data

- personal data
- identity
- username
- profile
- oversharing
- context

AI & fake media

- AI-generated
- deepfake
- source
- verify
- original
- evidence

Digital footprint

- digital footprint
- active
- passive
- permanent
- cookies
- tracking

Harm, contact & reporting

- cyberbullying
- bystander
- upstander
- block
- report
- warning signs
- age rating
- trusted adult

Passwords & accounts

- password
- passphrase
- two-step verification
- account
- reuse
- guessable

Your safety campaign

- audience
- purpose
- campaign
- message
- accessibility
- infographic

Cyber Security & Threats

Social engineering, malware and AI-powered scams

THE QUESTION THIS UNIT ANSWERS

“Who is trying to take it, and how do they do it?”

SIX BIG IDEAS

- 1 Attackers want money, data, disruption or reputation. Even your account has a market price.
- 2 People are the weakest link. No software stops someone who is manipulated into helping.
- 3 Your public footprint is the attacker’s research. It supplies the detail that makes a lie believable.
- 4 AI has removed the bad-spelling tell, and a familiar voice is no longer proof of identity.
- 5 Verify on a second channel *you* start. Never act on urgency alone; agree a family safe word.
- 6 Backups are what actually defeat ransomware, and passkeys beat SMS codes.

ANATOMY OF A PHISHING MESSAGE

FROM USI IT Support <support@usi-portal.co>¹

TO undisclosed recipients²

SUBJECT ACTION REQUIRED within 2 hours³

Dear Student,⁴

Your account storage is full and will be **deleted tonight**. Confirm your password now to keep your coursework.⁵

[Verify my account](#)⁶

Attached: account_form.zip⁷

- 1 Display name looks right; the real domain does not.
- 2 Sent to hundreds at once.
- 3 Manufactured urgency and a deadline.
- 4 Generic greeting, no name.
- 5 Asks for something no real service asks for.
- 6 Hover before you click: the link goes elsewhere.
- 7 Unexpected attachment.

Do not click. Do not reply. Report, then delete.

KEY VOCABULARY

Attackers & motive

cyber security

threat

attacker

motive

data value

confidentiality

integrity

availability

Social engineering

social engineering

pretext

urgency

authority

baiting

shoulder surfing

manipulation

Fake messages

phishing

spear phishing

smishing

domain

spoofing

hyperlink

indicator

Malware

malware

virus

worm

trojan

ransomware

spyware

patch

backup

AI-generated media

generative AI

training data

deepfake

voice cloning

provenance

watermark

reverse image search

amplification

Defending the account

credential stuffing

data breach

password manager

multi-factor authentication

passkey

permissions

harvesting

safe word

Cyber Security & Data Protection

System attacks, encryption, the law and synthetic identity

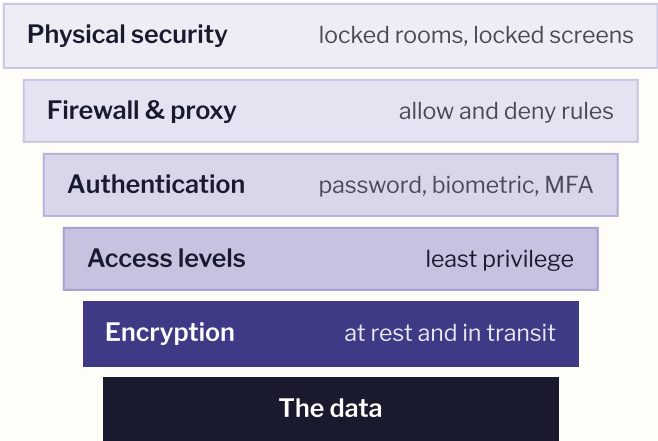
THE QUESTION THIS UNIT ANSWERS

“How are systems protected, what does the law require, and what is right?”

SEVEN BIG IDEAS

- 1
- Vulnerability, threat and risk are three different things. Know which one you are talking about.
- 2
- Every extra character multiplies the keyspace. That is why length beats complexity, in numbers.
- 3
- No single control is enough. Security is layered: defence in depth, and least privilege throughout.
- 4
- Encryption stops interception. It does not stop a stolen password or a phishing click.
- 5
- Data protection is law here: Qatar Law No. 13 of 2016, with GDPR as the international comparator.
- 6
- The liar’s dividend: once anything can be faked, the guilty dismiss real evidence as fake.
- 7
- Your prompt is data. Never put another person’s details into a public AI tool.

DEFENCE IN DEPTH



Keyspace: why length wins

- 4-digit PIN

$10^4 = 10,000$ combinations
- 8 characters

around 95^8 — roughly 6.6 quadrillion
- 4 random words

far larger still, and easier to remember

KEY VOCABULARY

Attacks on systems

- attack surface
- brute force
- dictionary attack
- DDoS
- interception
- vulnerability
- threat
- risk

Data protection & the law

- personal data
- consent
- data minimisation
- retention
- breach
- data subject
- rights
- GDPR

System defences

- firewall
- proxy server
- authentication
- biometrics
- access level
- least privilege
- defence in depth

Synthetic identity

- synthetic media
- liar’s dividend
- provenance
- content credentials
- defamation
- disinformation
- liability

Encryption

- encryption
- plaintext
- ciphertext
- key
- symmetric
- asymmetric
- HTTPS / TLS
- frequency analysis

AI, privacy & ethics

- prompt
- training data
- scraping
- anonymisation
- re-identification
- academic integrity
- computer misuse
- responsible disclosure