CHƯƠNG 2

INTERNET, LƯU TRỮ ĐÁM MÂY VÀ AN TOÀN THÔNG TIN

Giáo trình môn Tin học · Slide bài giảng

Trường Đại học Sân khấu - Điện ảnh Hà Nội
Biên soạn: ThS. Lê Khắc Tuấn

Mục tiêu chương

1	**Mạng và Internet**	Giải thích IP, DNS, HTTPS, băng thông, độ trễ; phân biệt thiết bị mạng và chuẩn Wi-Fi
2	**Tìm kiếm và kiểm chứng**	Tìm kiếm nâng cao, đánh giá nguồn bằng SIFT, nhận diện tin giả và deepfake
3	**Đám mây**	Lưu trữ, đồng bộ, chia sẻ, cộng tác; quy trình làm việc với file dung lượng lớn
4	**An ninh mạng**	Nhận biết mã độc, lừa đảo, tấn công phi kỹ thuật; bảo vệ thiết bị, tài khoản, dữ liệu
5	**Danh tính số và pháp luật**	Quản lý danh tính số; hiểu quy định về an ninh mạng và dữ liệu cá nhân

Cấu trúc nội dung chương

Nội dung chương

2.1 Mạng máy tính
2.2 Internet hoạt động như thế nào
2.3 Tìm kiếm và đánh giá thông tin
2.4 Lưu trữ đám mây
2.5 Giao tiếp trực tuyến
2.6 An toàn thông tin

Thực hành trên lớp (2 tiết)

BT1 Khám phá mạng và Internet
BT2 Kiểm chứng thông tin
BT3 Thiết lập đám mây cho dự án

Làm ở nhà

BT4 Rà soát bảo mật tài khoản
BT5 Trình quản lý mật khẩu
BT6 Bảo vệ thiết bị và dữ liệu cá nhân
Bài tập tìm hiểu: chọn 2 trong 7

2.1

Mạng máy tính

Khái niệm · Phân loại · Thiết bị mạng · Wi-Fi

Mạng máy tính là gì?

Mạng máy tính (computer network) là tập hợp các máy tính và thiết bị được kết nối với nhau để trao đổi dữ liệu và chia sẻ tài nguyên.

Ví dụ: Hàng chục người trong một studio cùng truy cập kho footage trên máy chủ, cùng chỉnh sửa một tài liệu Google Docs, gửi bản dựng cho khách hàng ở nước ngoài trong vài phút.

Chia sẻ: dữ liệu, máy in, ổ lưu trữ, phần mềm

Giao tiếp: email, chat, video call

Truy cập thông tin: web

Cộng tác từ xa: nhiều người, nhiều nơi

Phân phối tác phẩm: đến khán giả toàn cầu

Phân loại mạng theo phạm vi

Loại	Phạm vi	Ví dụ trong ngành sáng tạo
PAN	Vài mét quanh một người	Bluetooth tai nghe, AirDrop từ iPhone sang Mac, máy ảnh kết nối điện thoại
LAN	Một tòa nhà, một studio	Nhiều máy dựng dùng chung NAS chứa footage; mạng phòng máy của trường
WLAN	LAN không dây (Wi-Fi)	Wi-Fi trường quay, quán cà phê, nhà riêng
MAN	Một thành phố	Mạng tập đoàn truyền thông có nhiều trụ sở trong Hà Nội
WAN	Quốc gia, toàn cầu	Internet là WAN lớn nhất; mạng riêng của đài truyền hình nối các tỉnh

Nguyên tắc: Máy làm việc chính với file lớn nên cắm dây (Ethernet 1–10 Gbps, ổn định, độ trễ thấp); Wi-Fi dành cho thiết bị di động.

Thiết bị mạng thường gặp









- **Modem / ONT:** nhà mạng (Viettel, VNPT, FPT) cấp, đổi tín hiệu cáp quang thành tín hiệu mạng; cửa ngõ ra Internet.
- **Router:** chia Internet cho nhiều thiết bị, cấp IP nội bộ, tường lửa cơ bản, thường có Wi-Fi.
- **Switch:** mở rộng cổng có dây. Studio 10 máy dựng cần switch 16–24 cổng Gigabit hoặc 10 Gigabit để truy cập NAS nhanh.
- **Access Point:** phát Wi-Fi mở rộng vùng phủ; Mesh Wi-Fi cho nhà nhiều tầng, trường quay rộng.
- **Card mạng (NIC):** cổng RJ45 hoặc chip Wi-Fi; laptop mỏng cần adapter USB-C to Ethernet.
- **Cáp mạng:** Cat5e (1 Gbps), Cat6 (1–10 Gbps ngắn), Cat6a (10 Gbps). Studio nên đi Cat6a để chuẩn bị cho 10 Gbps.

Hình 2.1. (a) Modem · (b) Router Wi-Fi · (c) Switch 8 cổng · (d) Access point. Ảnh: Aravind Sivaraj, Evan-Amos, Zuzu, Sabbo91 (Wikimedia Commons, CC BY-SA / phạm vi công cộng).

Wi-Fi: chuẩn và băng tần

Chuẩn	Tên thương mại	Tốc độ tối đa	Ghi chú
802.11ac	Wi-Fi 5 (2014)	~1–3 Gbps	Phổ biến nhất hiện nay, băng tần 5 GHz
802.11ax	Wi-Fi 6 (2019)	~9,6 Gbps	Tốt khi nhiều thiết bị; Wi-Fi 6E thêm băng 6 GHz
802.11be	Wi-Fi 7 (2024)	~46 Gbps	Mới nhất, độ trễ rất thấp

2,4 GHz

Xuyên tường tốt, xa hơn, nhưng chậm và dễ nhiễu

5 GHz

Nhanh hơn, ít nhiễu, tầm ngắn hơn. Ưu tiên khi truyền file lớn

6 GHz

Wi-Fi 6E/7: nhanh nhất, tầm ngắn nhất

Bảo mật Wi-Fi

✗ WEP

Đã lỗi thời, phá được trong vài phút. Không bao giờ dùng.

✓ WPA2

An toàn và phổ biến. Dùng kèm mật khẩu mạnh.

✓ WPA3

Mới nhất, tốt nhất. Chọn nếu router hỗ trợ.

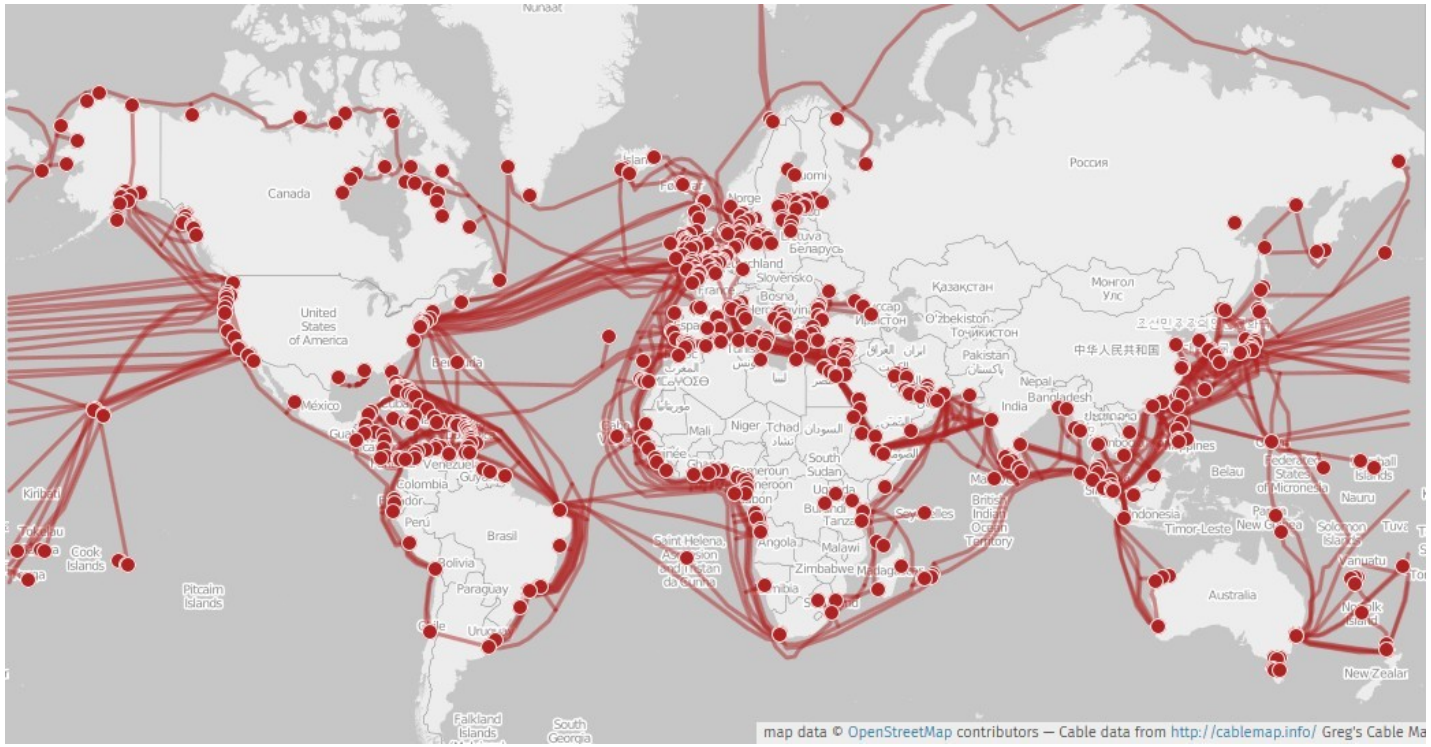
Lưu ý: Wi-Fi nhà riêng phải đặt mật khẩu WPA2/WPA3 mạnh và đổi mật khẩu quản trị router mặc định (admin/admin). Nhiều router bị chiếm quyền chỉ vì chủ nhà chưa từng đổi.

2.2

Internet hoạt động như thế nào?

IP · DNS · URL · HTTP/HTTPS · Băng thông · Trình duyệt · VPN

Internet: mạng của các mạng



- Hàng tỷ thiết bị kết nối qua cáp quang xuyên đại dương, vệ tinh và các trung tâm dữ liệu
- Không ai "sở hữu" Internet
- Vận hành nhờ các giao thức (protocol) chung mà mọi thiết bị đều tuân theo

Hình 2.2. Các tuyến cáp quang biển quốc tế. Dữ liệu: Greg Mahlknecht (cablemap.info), nền OpenStreetMap, CC BY-SA 2.0, Wikimedia Commons.

Địa chỉ IP

Mỗi thiết bị trên mạng có một địa chỉ IP duy nhất, như địa chỉ nhà để bưu điện gửi thư.

IPv4 (~4,3 tỷ địa chỉ, đã cạn)

192.168.1.15

IPv6 (340 tỷ tỷ tỷ tỷ địa chỉ)

2001:0db8:85a3::8a2e:0370:7334

IP nội bộ (private)

Router cấp trong nhà/studio: 192.168.x.x, 10.x.x.x. Chỉ có ý nghĩa trong mạng nội bộ.

IP công cộng (public)

Nhà mạng cấp cho router; cả Internet nhìn thấy. Tiết lộ vị trí đại khái và nhà mạng.

IP tĩnh / động

Hầu hết là IP động (đổi mỗi lần kết nối). Server, NAS truy cập từ xa dùng IP tĩnh hoặc DDNS.

DNS: danh bạ của Internet

Gõ youtube.com › **Máy hỏi máy chủ DNS: "youtube.com ở đâu?"** › **DNS trả lời IP 142.250.190.14** › **Trình duyệt kết nối đến IP đó**

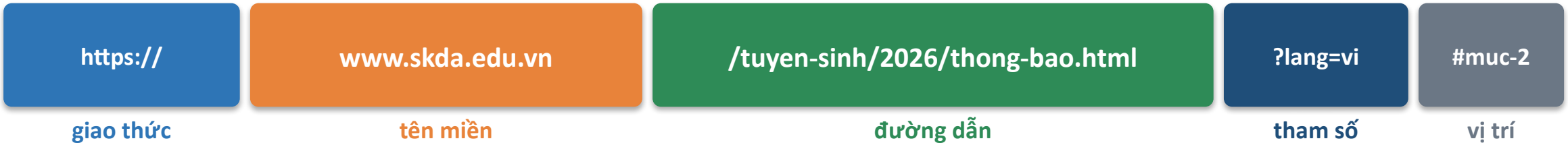
Toàn bộ mất vài mili giây. Tên miền www.skda.edu.vn đọc từ phải sang trái:

.vn	.edu	skda	www
quốc gia Việt Nam	giáo dục	tên tổ chức	tên máy chủ

Mẹo: Mặc định dùng DNS của nhà mạng. Có thể đổi sang DNS công cộng: Google 8.8.8.8 · Cloudflare 1.1.1.1 · Quad9 9.9.9.9 (chặn tên miền độc hại). Đổi DNS cũng là cách xử lý khi "có mạng nhưng không vào được web".

Web và URL

URL (Uniform Resource Locator) là địa chỉ đầy đủ của một tài nguyên trên web:



Ghi nhớ: Tên miền là phần quan trọng nhất để nhận biết trang web thật hay giả.

- **World Wide Web (WWW):** một dịch vụ chạy trên Internet (bên cạnh email, FTP, game online…).
- **Web gồm:** các trang HTML, liên kết bằng hyperlink, truy cập bằng trình duyệt.

HTTP và HTTPS

HTTP

Truyền dữ liệu dạng văn bản thuần. Ai ở giữa (quán cà phê, nhà mạng, hacker) cũng đọc được.

HTTPS

Mã hóa toàn bộ dữ liệu bằng chứng chỉ SSL/TLS; trình duyệt hiển thị biểu tượng ổ khóa.

Quy tắc: Không bao giờ nhập mật khẩu, thông tin thẻ trên trang http:// không có ổ khóa.

Cẩn thận: Có ổ khóa không có nghĩa trang web đáng tin. Trang lừa đảo cũng dùng được HTTPS. Ổ khóa chỉ bảo đảm mã hóa, không bảo đảm người nhận là ai.

Băng thông, tốc độ và độ trễ

Băng thông (Bandwidth)

Lượng dữ liệu tối đa truyền mỗi giây, đo bằng Mbps hoặc Gbps. Gói cáp quang gia đình phổ biến 150 Mbps – 1 Gbps.

Tốc độ thực tế (Throughput)

Luôn thấp hơn băng thông. Đo bằng speedtest.net hoặc fast.com. Phân biệt download và upload: upload thấp ảnh hưởng việc gửi video.

Độ trễ (Latency / Ping)

Thời gian tín hiệu đi và về, đo bằng mili giây. Quan trọng với video call, game. Dưới 50 ms là tốt.

Quy đổi cần nhớ: 8 bit = 1 byte. Mạng đo bằng bit (Mbps), file đo bằng byte (MB).

100 Mbps

lý thuyết 12,5 MB/s
thực tế ≈ 10 MB/s

5 GB, upload 50 Mbps

≈ 6 MB/s
mất khoảng 14 phút

5 GB, upload 10 Mbps

mất hơn 1 giờ

Trình duyệt web

Chrome (~65% thị phần) · Edge (mặc định trên Windows) · Safari · Firefox (riêng tư) · Brave (chặn quảng cáo sẵn)

Phím tắt	Chức năng
Ctrl + T / Ctrl + W	Mở / đóng tab
Ctrl + Tab	Chuyển tab
Ctrl + Shift + T	Mở lại tab vừa đóng
Ctrl + D	Đánh dấu trang (bookmark)
Ctrl + H	Lịch sử duyệt web
Ctrl + Shift + Delete	Xóa lịch sử và cache
Ctrl + Shift + N	Chế độ ẩn danh
F12	Developer Tools

- **Tab:** dùng nhóm tab (tab groups) để tổ chức theo dự án.
- **Cache:** bản sao tạm giúp tải nhanh hơn; xóa khi máy dùng chung hoặc trang lỗi.
- **Ẩn danh:** không lưu lịch sử trên máy, nhưng KHÔNG ẩn danh với nhà mạng và trang web.
- **Extension:** uBlock Origin, Bitwarden, Grammarly. Extension lạ có thể đọc mọi thứ người học gõ.
- **Đồng bộ:** đăng nhập Google/Microsoft để đồng bộ bookmark, mật khẩu, tab giữa các thiết bị.
- **F12:** xem mã nguồn trang, kiểm tra tốc độ tải, tải ảnh/video từ trang.

VPN: mạng riêng ảo

VPN tạo một "đường hầm" mã hóa giữa thiết bị và máy chủ VPN. Trang web đích chỉ thấy IP của máy chủ VPN, không thấy IP thật của người học.

1. Bảo vệ dữ liệu khi dùng Wi-Fi công cộng
2. Truy cập mạng nội bộ công ty/trường từ xa
3. Truy cập dịch vụ giới hạn theo khu vực (một số kho nhạc, footage chỉ mở ở nước ngoài)
4. Bảo vệ riêng tư khỏi nhà mạng theo dõi

Lưu ý: VPN miễn phí thường bán dữ liệu người dùng hoặc chèn quảng cáo. VPN uy tín: Proton VPN (có gói miễn phí tử tế), Mullvad, NordVPN, ExpressVPN. VPN không giúp ẩn danh hoàn toàn và không phải công cụ để vi phạm pháp luật.

2.3

Tìm kiếm và đánh giá thông tin

Toán tử tìm kiếm · AI · SIFT · Tin giả và deepfake

Toán tử tìm kiếm nâng cao

Toán tử	Chức năng	Ví dụ
"cụm từ"	Tìm chính xác cụm từ	"kỹ xảo điện ảnh" "giáo trình"
-từ	Loại trừ từ	premiere -adobe (tìm buổi ra mắt phim, không phải phần mềm)
site:	Chỉ tìm trong một trang	site:skda.edu.vn tuyển sinh
filetype:	Tìm loại file cụ thể	filetype:pdf storyboard template
OR	Hoặc	"color grading" OR "chỉnh màu"
*****	Ký tự đại diện	"đạo diễn * nổi tiếng"
intitle:	Từ trong tiêu đề	intitle:"free footage"
before: / after:	Giới hạn thời gian	AI video after:2025-01-01
define: / related:	Định nghĩa / trang tương tự	define:compositing · related:artgrid.io

Mẹo tìm kiếm và tìm kiếm với AI

Mẹo cho ngành sáng tạo

- Tìm tài nguyên có bản quyền rõ ràng: “royalty free”, “CC0”, “public domain”
- Tìm bằng tiếng Anh để có kết quả phong phú hơn
- Google Images › Tools › Usage rights › Creative Commons
- Tìm ngược bằng hình ảnh (Google Lens, TinEye) để tìm nguồn gốc ảnh hoặc kiểm tra ảnh bị chỉnh sửa

Tìm kiếm với AI

ChatGPT, Claude, Gemini, Perplexity, Copilot tổng hợp nhanh và trả lời trực tiếp.

Cảnh giác: AI có thể “ảo giác” (hallucination): bịa thông tin, trích dẫn, số liệu nghe rất thuyết phục nhưng sai. Dùng AI để định hướng; luôn kiểm chứng bằng nguồn gốc.

Phương pháp SIFT

Bốn bước nhanh để kiểm tra bất kỳ thông tin nào trên mạng (Mike Caulfield, 2019)

S

Stop

Dừng lại

Trước khi tin hoặc chia sẻ. Cảm xúc mạnh (phẫn nộ, sợ hãi) là dấu hiệu cần cảnh giác.

I

Investigate

Điều tra nguồn

Ai đăng? Tìm tên nguồn trên Wikipedia/Google. Tài khoản mới lập, ít theo dõi → nghi ngờ.

F

Find

Tìm nguồn khác

Báo lớn, cơ quan chính thức có đưa tin không? “Tin chấn động” chỉ có một nguồn → rất có thể giả.

T

Trace

Truy về gốc

Ảnh, video, trích dẫn hay bị cắt xén, lấy khỏi ngữ cảnh. Tìm bản gốc đầy đủ.

Mức độ tin cậy của nguồn thông tin

Mức	Loại nguồn	Ví dụ
Cao	Cơ quan chính phủ, tổ chức quốc tế, tạp chí khoa học bình duyệt, giáo trình, tài liệu chính thức của nhà sản xuất	moet.gov.vn, unesco.org, hướng dẫn Adobe/Blackmagic
Trung bình	Báo chí chính thống, chuyên gia có tên tuổi, diễn đàn chuyên ngành uy tín	VnExpress, Tuổi Trẻ, No Film School
Thấp	Blog cá nhân, mạng xã hội, trang tổng hợp, video không rõ tác giả	Bài đăng Facebook, TikTok, trang "tin nhanh" không có tòa soạn
Rất thấp	Trang giả mạo, tài khoản ẩn danh, nội dung AI không kiểm chứng	Tên miền gần giống báo lớn (vnexpres.com), nhóm chat lan truyền

Tài liệu học thuật, tiêu chí CRAAP: Currency (thời điểm) · Relevance (liên quan) · Authority (thẩm quyền) · Accuracy (chính xác) · Purpose (mục đích)

Tin giả và deepfake

Tin giả

Thông tin sai lệch lan truyền vô tình (misinformation) hoặc cố ý (disinformation). Dấu hiệu: tiêu đề giật gân, kêu gọi "chia sẻ ngay", không tác giả/ngày tháng/nguồn, tên miền lạ.

Deepfake

Video, ảnh, giọng nói do AI tạo hoặc chỉnh sửa để trông như thật. Có ứng dụng chính đáng trong điện ảnh, nhưng bị lạm dụng để lừa đảo, tống tiền, bôi nhọ.

Dấu hiệu nhận biết deepfake

- Môi không khớp âm thanh, chớp mắt bất thường
- Viền mặt, tóc, tai nhòe khi quay đầu
- Ánh sáng trên mặt không khớp nền
- Giọng thiếu ngữ điệu, không có tiếng thở; tay biến dạng

Cách xác minh

- Tìm ngược ảnh/khung hình (Google Lens, TinEye)
- Kiểm tra video có trên kênh chính thức không
- Công cụ: Deepware Scanner, Intel FakeCatcher
- Quan trọng nhất: gọi điện xác minh trực tiếp khi có yêu cầu liên quan đến tiền

2.4

Lưu trữ đám mây

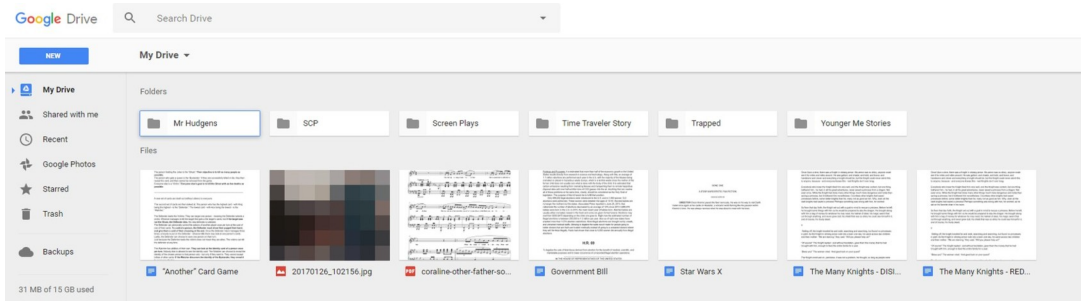
Dịch vụ · Đồng bộ và sao lưu · Chia sẻ · Quy trình file lớn

Lưu trữ đám mây và các dịch vụ phổ biến

Điện toán đám mây cung cấp lưu trữ, xử lý, phần mềm qua Internet theo nhu cầu; file được sao chép vào nhiều máy chủ ở nhiều nơi nên gần như không bao giờ mất.

Dịch vụ	Miễn phí	Trả phí (2026)	Đặc điểm
Google Drive	15 GB (chung Gmail, Photos)	100 GB ~45.000đ/tháng; 2 TB ~220.000đ	Tích hợp Docs/Sheets/Slides; phổ biến nhất ở Việt Nam
OneDrive	5 GB	100 GB ~45.000đ; 1 TB kèm Microsoft 365	Tích hợp Windows/Office; Files On-Demand
Dropbox	2 GB	2 TB ~12 USD/tháng	Đồng bộ nhanh và tin cậy; Dropbox Replay
iCloud Drive	5 GB	50 GB ~25.000đ; 2 TB ~250.000đ	Hệ sinh thái Apple; tự sao lưu iPhone
Frame.io	2 GB	Kèm Creative Cloud	Duyệt video: nhận xét theo timecode
WeTransfer / Smash	2 GB/lần / không giới hạn	Pro ~10 USD	Gửi file lớn một lần, liên kết hết hạn sau 7 ngày

Đồng bộ và sao lưu: hai khái niệm khác nhau



Hình 2.3. Giao diện web Google Drive (bản 2017, bố cục tương tự hiện nay). Ảnh: Hazumane, CC BY-SA 4.0, Wikimedia Commons (đã chỉnh sửa).

Đồng bộ (Sync)

Thư mục trên máy và trên đám mây luôn giống nhau, hai chiều. Xóa ở máy → xóa trên đám mây. Tiện cho nhiều thiết bị, nhưng không phải backup.

Sao lưu (Backup)

Sao chép một chiều từ máy lên nơi lưu trữ, giữ nhiều phiên bản. Xóa ở máy không ảnh hưởng bản backup. Dùng chế độ Backup của Google Drive Desktop, OneDrive, hoặc dịch vụ chuyên (Backblaze).

Quy tắc 3-2-1: Đám mây đóng vai trò bản sao "ở nơi khác" trong quy tắc 3-2-1. Để đúng nghĩa backup, hãy giữ thêm một bản trên ổ cứng ngoài không đồng bộ.

Ứng dụng đồng bộ trên máy tính

Stream / Files On-Demand

File hiện trong File Explorer nhưng chỉ tải khi mở. Tiết kiệm ổ cứng, hợp laptop SSD nhỏ. Biểu tượng đám mây = chưa tải; dấu tích xanh = đã có trên máy.

Mirror / Always keep on this device

Tải toàn bộ về máy, làm việc offline được. Cần ổ cứng đủ lớn.

Cảnh báo: Không mở file dự án Premiere / DaVinci / After Effects trực tiếp từ thư mục đang đồng bộ đám mây: phần mềm ghi file liên tục, đồng bộ liên tục gây xung đột, hỏng file dự án.

Cách đúng: Làm việc trên SSD nội bộ, sao chép hoặc backup lên đám mây theo lịch.

Chia sẻ và phân quyền

Quyền	Người nhận có thể	Dùng khi
Viewer (Xem)	Xem, tải về (có thể tắt tải)	Gửi bản dựng cho khách duyệt, nộp bài
Commenter (Nhận xét)	Xem + thêm nhận xét, không sửa	Duyệt kịch bản, lấy ý kiến
Editor (Chỉnh sửa)	Xem, sửa, xóa, chia sẻ tiếp	Nhóm cùng làm dự án

Restricted

Chỉ người được thêm email

Anyone with the link

Ai có liên kết đều vào được; có thể bị chuyển tiếp ngoài ý muốn

Trong tổ chức

Chỉ tài khoản cùng trường/công ty

Nguyên tắc: Dữ liệu nhạy cảm chỉ chia sẻ Restricted, đặt ngày hết hạn; thu hồi quyền khi dự án kết thúc.

Quy trình làm việc với file lớn

1 Footage gốc

SSD nội bộ + ổ ngoài; không đưa lên đám mây trừ khi có gói lớn

2 Proxy

Bản video độ phân giải thấp (720p, ~1/10 dung lượng) để dựng và chia sẻ

3 File dự án

.prproj, .drp chỉ vài MB, đưa lên đám mây, đồng bộ nhóm

4 Bản duyệt

Xuất H.264 1080p nhỏ, gửi qua Frame.io, Drive, YouTube unlisted

5 Bản cuối

Chất lượng cao, gửi qua WeTransfer/Smash hoặc giao ổ cứng

6 Lưu trữ

Archive vào ổ ngoài + cloud archive (Google One 2 TB, Backblaze B2) khi kết thúc dự án

2.5

Giao tiếp trực tuyến

Email chuyên nghiệp · Nền tảng họp trực tuyến

Email chuyên nghiệp

Địa chỉ

nghiêm túc: nguyenvana@gmail.com hoặc email trường (.edu.vn), không phải cobebutchi2005@… Dùng email trường cho việc học

Tiêu đề

rõ ràng: [Tin học cơ bản] Nộp bài tập buổi 2 — Nguyễn Văn A — Lớp DD45. Không để trống hoặc “Hỏi”, “Gửi thầy”

Cấu trúc

Lời chào (Kính gửi thầy/cô + tên) → giới thiệu ngắn → nội dung chính → cảm ơn → chữ ký (họ tên, lớp, số điện thoại)

Đính kèm

đặt tên đúng quy ước; file > 25 MB gửi liên kết Drive; nói rõ trong nội dung có đính kèm gì

Cc / Bcc

Cc để người khác biết; Bcc khi gửi nhiều người mà không lộ email của nhau (ví dụ thông báo cho cả lớp)

Thói quen

trả lời trong 24 giờ; Reply All cẩn thận; đọc lại trước khi gửi; không viết email khi đang tức giận

Nền tảng giao tiếp và họp trực tuyến

Nền tảng	Đặc điểm	Phù hợp
Zalo	Phổ biến nhất Việt Nam, nhóm, gọi video, gửi file 1 GB	Liên lạc nhanh, nhóm lớp
Microsoft Teams	Tích hợp Office 365, kênh theo dự án, họp, lưu file	Trường/doanh nghiệp dùng Microsoft
Google Meet	Đơn giản, tích hợp Calendar, Gmail	Họp nhanh, dạy học
Zoom	Ổn định, breakout room, ghi hình	Hội thảo, lớp đông
Slack / Discord	Kênh chủ đề, tích hợp công cụ	Nhóm sản xuất, cộng đồng
Telegram	Nhanh, gửi file 2 GB, bot, kênh	Cộng đồng, chia sẻ tài nguyên

Nghi thức họp: Kiểm tra mic, camera, mạng trước 5 phút · tắt mic khi không nói · bật camera khi có thể · đặt tên hiển thị đúng (Họ tên — Lớp) · nền gọn gàng hoặc dùng nền ảo · không làm việc khác khi họp · ghi chú và tóm tắt sau họp.

2.6

An toàn thông tin

Mối đe dọa · Mật khẩu · 2FA · Thiết bị · Dữ liệu cá nhân · Pháp luật

Tài sản cần bảo vệ

An toàn thông tin là bảo vệ dữ liệu và hệ thống khỏi truy cập trái phép, phá hoại, đánh cắp.

1 Tài khoản

Email, mạng xã hội, ngân hàng, Adobe, Google Drive

2 Dữ liệu

Dự án, portfolio, footage khách hàng

3 Thiết bị

Laptop, điện thoại, ổ cứng

4 Danh tính số

Hình ảnh, uy tín trên mạng

Thực tế: Người học là nhóm bị nhắm đến nhiều với các thủ đoạn “việc nhẹ lương cao”, “cộng tác viên”, “trúng thưởng”, giả danh công an, giáo viên. Thiệt hại do lừa đảo trực tuyến năm 2025 ước tính hàng nghìn tỷ đồng.

Mã độc (Malware)

Loại	Hoạt động	Lây qua
Virus	Gắn vào file/chương trình, lây khi chạy, phá dữ liệu	File tải về, USB, email đính kèm
Trojan	Giả dạng phần mềm hữu ích, mở cửa hậu cho mã độc	Phần mềm crack, “tool hack”
Ransomware	Mã hóa toàn bộ file, đòi tiền chuộc để giải mã	Email phishing, crack, lỗ hổng chưa vá
Spyware / Keylogger	Ghi phím gõ, chụp màn hình, đánh cắp mật khẩu	Extension lạ, ứng dụng không rõ nguồn
Adware	Hiện quảng cáo, đổi trang chủ, theo dõi thói quen	Phần mềm miễn phí đi kèm
Cryptojacking	Dùng máy đào tiền ảo: máy chậm, nóng, tốn điện	Phần mềm crack, trang web độc

Ransomware: Một buổi sáng toàn bộ dự án 3 tháng bị mã hóa, màn hình đòi 500 USD Bitcoin. Không có backup = mất trắng. Phòng ngừa duy nhất: backup 3-2-1 với ít nhất một bản không kết nối mạng.

Phishing và tấn công phi kỹ thuật

Phishing: lừa người dùng tự nộp thông tin (mật khẩu, mã OTP, số thẻ) bằng cách giả mạo tổ chức uy tín.

Email phishing

"Tài khoản Google sắp bị khóa, nhấn để xác minh" → trang đăng nhập giả

Smishing (SMS)

"Bạn có bưu phẩm chưa nhận, truy cập link" giả danh bưu điện, ngân hàng, thuế

Vishing (gọi điện)

Giả danh công an, ngân hàng, giáo viên, kèm deepfake giọng nói; tạo hoảng sợ

Lừa đảo việc làm

"Cộng tác viên chốt đơn", "like video nhận tiền": trả tiền thật rồi yêu cầu nạp tiền

Tình cảm, đầu tư

Làm quen, xây dựng tình cảm, rủ đầu tư tiền ảo, forex trên sàn giả

Giả mạo ngành sáng tạo

"Nhãn hàng hợp tác, gửi CCCD"; "Casting phim, đóng phí hồ sơ"; email giả Adobe

Nhận biết phishing

Tạo khẩn cấp, sợ hãi (“trong 24 giờ”, “ngay lập tức”)

Địa chỉ gửi lạ hoặc gần giống thật (support@g00gle.com)

Liên kết hiển thị khác liên kết thật (rê chuột để xem)

Lỗi chính tả, xưng hô chung chung (“Kính gửi khách hàng”)

Hỏi mật khẩu, OTP, thông tin thẻ: tổ chức thật không bao giờ hỏi

Đính kèm .exe, .zip, .docm bất ngờ; “quá tốt để là thật”

Nguyên tắc vàng: Khi nghi ngờ, không nhấn liên kết trong email/tin nhắn: tự gõ địa chỉ chính thức hoặc mở ứng dụng. Có yêu cầu liên quan đến tiền: gọi lại số điện thoại chính thức (không phải số trong tin nhắn). Không có cơ quan công an nào làm việc qua điện thoại và yêu cầu chuyển tiền.

Các mối đe dọa khác và Wi-Fi công cộng

Dò mật khẩu

Brute force, credential stuffing: dùng mật khẩu lộ ở trang A thử trang B. Kiểm tra tại haveibeenpwned.com.

Wi-Fi giả (Evil twin)

Wi-Fi tên giống quán cà phê, kết nối là bị đọc dữ liệu không mã hóa.

Chiếm tài khoản MXH

Facebook bị hack → nhắn bạn bè vay tiền. Rất phổ biến ở Việt Nam.

Lộ dữ liệu từ dịch vụ

Trang đã đăng ký bị hack, lộ email + mật khẩu của hàng triệu người.

Khi buộc phải dùng Wi-Fi công cộng

- Ưu tiên 4G/5G cá nhân cho giao dịch quan trọng · xác nhận tên Wi-Fi với nhân viên · chỉ truy cập HTTPS · bật VPN
- Không đăng nhập ngân hàng, không nhập thẻ · tắt chia sẻ file (Windows: đặt mạng là Public) · tắt Wi-Fi/Bluetooth khi không dùng · tắt tự động kết nối Wi-Fi mở

Mật khẩu mạnh

Mật khẩu	Thời gian phá (2026)	Nhận xét
123456	Tức thì	Phổ biến nhất thế giới
tuan2005	Tức thì	Tên + năm sinh, có trong từ điển
Tuan@2005	Vài phút	Thêm ký tự đặc biệt chưa đủ
Xk7#mP2$vQ9!	Hàng thế kỷ	Mạnh nhưng không nhớ nổi
SenTanNoHoaMuaThu2026!	Hàng triệu năm	Cụm từ dài, dễ nhớ, rất mạnh

Nguyên tắc

- **Dài:** tối thiểu 12 ký tự, tốt nhất 16+; dùng cụm từ (passphrase)
- **Mỗi tài khoản một mật khẩu:** quan trọng nhất. Không chứa thông tin cá nhân, không ghi giấy dán màn hình

Trình quản lý mật khẩu

Tạo mật khẩu ngẫu nhiên rất mạnh cho từng trang, lưu mã hóa, tự điền khi đăng nhập. Người học chỉ nhớ một mật khẩu chủ (master password).

Bitwarden

Miễn phí, mã nguồn mở. Khuyến nghị.

1Password / Proton Pass

Các lựa chọn khác cùng nhóm.

Trình quản lý tích hợp sẵn

Google Password Manager, iCloud Keychain: tiện nhưng gắn với một hệ sinh thái.

Thực hành: Master password dạng passphrase 4–5 từ; kiểm tra email trên haveibeenpwned.com, nếu bị lộ thì đổi mật khẩu tài khoản đó ngay.

Xác thực hai yếu tố (2FA)

Thêm một bằng chứng ngoài mật khẩu: thứ người dùng biết + thứ người dùng có (điện thoại, khóa vật lý) hoặc thứ người dùng là (vân tay, khuôn mặt).

Phương thức	An toàn	Tiện lợi	Ghi chú
SMS OTP	Thấp	Cao	Bị chiếm SIM, bị lừa đọc OTP. Tốt hơn không có
Ứng dụng xác thực	Cao	Cao	Google/Microsoft Authenticator; mã 6 số đổi mỗi 30 giây. Khuyến nghị
Thông báo đẩy	Cao	Rất cao	Cẩn thận "MFA fatigue": kẻ xấu spam thông báo đến khi bấm nhầm
Khóa vật lý (FIDO2)	Rất cao	Trung bình	YubiKey, Google Titan; chống phishing tuyệt đối
Passkey	Rất cao	Rất cao	Chuẩn mới (2023+), thay mật khẩu bằng sinh trắc học trên thiết bị

Bật 2FA ngay cho: Email chính · ngân hàng · Facebook/Instagram/TikTok · Google Drive/iCloud · Adobe/Steam. Lưu backup codes ở nơi an toàn.

Bảo vệ thiết bị

Cập nhật

Bật cập nhật tự động. WannaCry 2017 lây 200.000 máy vì chưa vá lỗi

Chống virus

Windows Security có sẵn, đủ tốt. Chỉ cài một phần mềm chống virus

Tường lửa

Windows Firewall bật mặc định: giữ nguyên

Mã hóa ổ đĩa

BitLocker / Device Encryption (Windows), FileVault (macOS)

Khóa màn hình

Tự khóa sau 5 phút; Win + L mỗi khi rời máy

Nguồn phần mềm

Chỉ tải từ nguồn chính thức. Không crack: ~90% chứa mã độc

USB lạ

Không cắm USB không rõ nguồn; tắt AutoPlay

Tìm và xóa từ xa

Bật Find My Device / Find My để khóa, xóa dữ liệu khi mất máy

Dữ liệu cá nhân và danh tính số

Chia sẻ tối thiểu

- Cửa hàng bán áo không cần CCCD và ngày sinh
- Không đăng ảnh CCCD, thẻ, vé, hóa đơn có mã QR (kể cả story)
- Tắt định vị (EXIF) khi đăng ảnh
- Dùng email phụ: tuan+shopee@gmail.com

Kiểm soát riêng tư

- Mạng xã hội: bài viết mặc định “Bạn bè”, rà soát Apps and Websites
- Điện thoại: xem quyền từng ứng dụng, từ chối quyền không cần
- Google: myaccount.google.com › Data & privacy
- Trình duyệt: chặn cookie bên thứ ba

Danh tính số

- Dấu chân số gần như không xóa được
- Nhà tuyển dụng, ban tuyển sinh tìm tên người học trên Google trước
- Tự tìm tên mình (kèm ngoặc kép) định kỳ
- Tách tài khoản công việc và cá nhân

Khi sự cố xảy ra

Tình huống	Hành động ngay
Nhấn liên kết phishing, đã nhập mật khẩu	Đổi mật khẩu từ thiết bị khác → bật 2FA → kiểm tra đăng nhập lạ → đăng xuất mọi thiết bị → đổi mật khẩu các tài khoản dùng chung
Tài khoản Facebook/Gmail bị chiếm	Dùng chức năng khôi phục → báo bạn bè đừng chuyển tiền → đổi mật khẩu, bật 2FA, xem lại ứng dụng đã cấp quyền
Máy nhiễm mã độc / ransomware	Ngắt mạng ngay → không trả tiền chuộc → quét bằng Windows Security/Malwarebytes → khôi phục từ backup → nếu nghiêm trọng: cài lại Windows
Mất laptop / điện thoại	Find My Device khóa/xóa từ xa → đổi mật khẩu email, ngân hàng, đám mây → báo nhà mạng khóa SIM → báo công an → thông báo trường/công ty nếu có dữ liệu tổ chức
Bị lừa chuyển tiền	Gọi ngân hàng phong tỏa giao dịch → giữ bằng chứng → trình báo công an hoặc canhbaolua.vn, chongluadao.vn
Bị lộ ảnh/thông tin nhạy cảm	Không hoảng, không trả tiền tống tiền → chụp bằng chứng → báo nền tảng gỡ nội dung → trình báo công an → tìm hỗ trợ từ người thân, trường, đường dây nóng

Pháp luật Việt Nam về an ninh mạng và dữ liệu cá nhân

Luật An ninh mạng 2018	Hiệu lực 01/01/2019. Cấm đăng tin sai sự thật, xúc phạm danh dự, phát tán mã độc, chiếm đoạt tài khoản, tấn công mạng; yêu cầu doanh nghiệp bảo vệ dữ liệu người dùng.
Nghị định 13/2023/NĐ-CP	Hiệu lực 01/07/2023. Chủ thể dữ liệu có quyền được biết, đồng ý, truy cập, rút lại đồng ý, xóa, hạn chế, phản đối, khiếu nại, bồi thường.
Luật Bảo vệ dữ liệu cá nhân 2025	Quốc hội thông qua tháng 6/2025, hiệu lực 01/01/2026. Nâng Nghị định 13 thành luật, tăng mức xử phạt, quy định trách nhiệm khi dùng AI xử lý dữ liệu.
Nghị định 15/2020/NĐ-CP	Sửa đổi bởi 14/2022. Phạt 10–20 triệu đồng với hành vi cung cấp, chia sẻ thông tin giả mạo, sai sự thật trên mạng xã hội; xúc phạm uy tín cơ quan, danh dự cá nhân.
Bộ luật Hình sự 2015 (sửa đổi 2017)	Điều 174 lừa đảo chiếm đoạt tài sản; 288 đưa/sử dụng trái phép thông tin mạng; 289 xâm nhập trái phép mạng máy tính; 290 sử dụng mạng máy tính chiếm đoạt tài sản. Phạt tù đến 20 năm.

Lưu ý: Quay phim, chụp ảnh người khác rồi đăng lên mạng = xử lý dữ liệu cá nhân của họ: cần sự đồng ý, nhất là mục đích thương mại. Dùng AI tạo hình ảnh giống người thật có thể vi phạm quyền hình ảnh (Điều 32 Bộ luật Dân sự).

TH

Thực hành và củng cố

Bài tập thực hành · Tóm tắt · Câu hỏi ôn tập · Bài tập tìm hiểu

Thực hành trên lớp (BT1 – BT3)

BT1

Khám phá mạng và Internet (15 phút)

ipconfig: IP nội bộ, gateway, DNS · tìm IP công cộng bằng "what is my ip" · nslookup skda.edu.vn · ping google.com đo độ trễ · speedtest.net đo download/upload/ping · tính thời gian gửi file 5 GB với upload vừa đo · chụp ảnh từng bước

BT2

Kiểm chứng thông tin (15 phút)

Giảng viên cung cấp 3 tin (1 thật, 1 giả, 1 nửa thật nửa giả): áp dụng SIFT cho từng tin, ghi từng bước điều tra, công cụ đã dùng (tìm ngược ảnh, kiểm tra tên miền, tìm nguồn khác) và kết luận; bảng 3 cột Tin / Các bước SIFT / Kết luận

BT3

Thiết lập đám mây cho dự án (15 phút)

Đưa cấu trúc thư mục dự án (BT2 chương 1) lên Google Drive/OneDrive · cài ứng dụng Desktop, chọn Stream · chia sẻ 01_PreProduction quyền Commenter, 05_Project_Files quyền Editor với 1 bạn cùng lớp; bạn thêm 1 nhận xét và 1 file · chụp ảnh cài đặt chia sẻ và kết quả · sau đó thu hồi quyền

Bài tập làm ở nhà (BT4 – BT5)

BT4

Rà soát bảo mật tài khoản (bắt buộc)

Tài khoản Google chính: myaccount.google.com > Security. (a) Chạy Security Checkup. (b) “Your devices”: đăng xuất thiết bị lạ. (c) Bật 2-Step Verification bằng Google Authenticator hoặc Microsoft Authenticator (không dùng SMS). (d) Tải và lưu Backup codes ở nơi an toàn. (e) “Third-party apps with account access”: thu hồi ứng dụng không dùng. Chụp ảnh kết quả (che thông tin nhạy cảm). Lặp lại (c) cho Facebook.

BT5

Triển khai trình quản lý mật khẩu

Cài Bitwarden (miễn phí) trên máy tính và điện thoại, cài extension trình duyệt. Tạo master password dạng passphrase 4–5 từ. Nhập/tạo mới mật khẩu cho ít nhất 5 tài khoản, dùng trình tạo mật khẩu ngẫu nhiên 16+ ký tự cho từng tài khoản. Kiểm tra email trên haveibeenpwned.com; nếu bị lộ, đổi mật khẩu tài khoản đó ngay. Viết 5–7 câu về trải nghiệm và kế hoạch chuyển toàn bộ tài khoản sang password manager.

Bài tập làm ở nhà (BT6) và tiêu chí đánh giá

BT6

Bảo vệ thiết bị và dữ liệu cá nhân

(a) Windows: kiểm tra Windows Update, Windows Security (quét toàn bộ), bật Device Encryption/BitLocker, tự khóa màn hình 5 phút, bật Find My Device. macOS: FileVault, Find My.
(b) Điện thoại: rà soát quyền ứng dụng (vị trí, micro, camera, danh bạ), thu hồi quyền không cần thiết cho ít nhất 3 ứng dụng.
(c) Facebook: bài viết mặc định Bạn bè, ẩn danh sách bạn bè và số điện thoại, xem lại Apps and Websites.
(d) Tự tìm tên mình trên Google (có ngoặc kép), ghi lại 5 kết quả đầu, nhận xét danh tính số. Chụp ảnh từng bước (che thông tin nhạy cảm), viết báo cáo 10 dòng.

Tiêu chí: Đúng và đủ yêu cầu 40% · Áp dụng đúng kiến thức, công cụ 30% · Trình bày rõ, ảnh chụp đầy đủ, có nhận xét cá nhân 20% · Đúng hạn, đúng định dạng 10%

Lưu ý: Bài tập chương 2 tính vào điểm Bài tập thường xuyên (20%). BT2 (kiểm chứng thông tin) và BT4 (bảo mật tài khoản) là bắt buộc.

Tóm tắt chương

Mạng và Internet	PAN/LAN/WAN; IP, DNS, URL; HTTPS mã hóa nhưng không bảo đảm đáng tin; Mbps ≠ MB (chia 8); VPN trên Wi-Fi công cộng
Thông tin	Toán tử tìm kiếm; SIFT: Stop, Investigate, Find, Trace; AI có thể ảo giác; deepfake: xác minh bằng cách gọi điện trực tiếp
Đám mây	Đồng bộ ≠ backup; không mở file dự án từ thư mục đồng bộ; proxy → dự án → duyệt → bản cuối → lưu trữ
Email	Địa chỉ nghiêm túc, tiêu đề rõ, cấu trúc đủ, file đặt tên đúng, Bcc khi gửi nhiều người
An toàn thông tin	Ransomware, phishing; không crack, không nhấn liên kết lạ, không đọc OTP cho ai; mật khẩu dài, mỗi tài khoản một mật khẩu; 2FA bằng ứng dụng; cập nhật, mã hóa ổ; chia sẻ tối thiểu
Pháp luật	Luật An ninh mạng 2018, Nghị định 13/2023, Luật Bảo vệ dữ liệu cá nhân 2025

Thuật ngữ cần nhớ: mạng và Internet

Thuật ngữ	Giải nghĩa
LAN / WAN	Mạng cục bộ / Mạng diện rộng
Router / Switch / Access Point	Bộ định tuyến / Bộ chuyển mạch / Điểm phát Wi-Fi
WPA2 / WPA3	Chuẩn bảo mật Wi-Fi hiện hành
IP Address	Địa chỉ định danh thiết bị trên mạng (IPv4: 192.168.1.1)
DNS	Hệ thống dịch tên miền thành địa chỉ IP
URL / Domain	Địa chỉ web đầy đủ / Tên miền
HTTP / HTTPS	Giao thức web không mã hóa / có mã hóa (SSL/TLS)
Bandwidth / Latency	Băng thông (Mbps) / Độ trễ (ms)
VPN	Mạng riêng ảo — đường hầm mã hóa

Thuật ngữ cần nhớ: thông tin, đám mây, danh tính

Thuật ngữ	Giải nghĩa
SIFT	Stop, Investigate, Find, Trace — phương pháp kiểm chứng thông tin
Misinformation / Disinformation	Thông tin sai vô tình / cố ý
Deepfake	Nội dung giả do AI tạo (mặt, giọng nói)
Cloud Storage	Lưu trữ đám mây
Sync / Backup	Đồng bộ hai chiều / Sao lưu một chiều có phiên bản
Proxy (video)	Bản video độ phân giải thấp để dựng nhanh
Digital Identity / Footprint	Danh tính số / Dấu chân số
Nghị định 13/2023/NĐ-CP	Quy định bảo vệ dữ liệu cá nhân tại Việt Nam

Thuật ngữ cần nhớ: an toàn thông tin

Thuật ngữ	Giải nghĩa
Malware / Ransomware / Trojan	Mã độc / Mã độc tống tiền / Mã độc giả dạng phần mềm hữu ích
Phishing / Smishing / Vishing	Lừa đảo qua email / SMS / gọi điện
Social Engineering	Tấn công phi kỹ thuật — lừa con người thay vì hack máy
Passphrase	Mật khẩu dạng cụm từ dài
Password Manager	Trình quản lý mật khẩu (Bitwarden, 1Password)
2FA / MFA	Xác thực hai / đa yếu tố
Authenticator App	Ứng dụng tạo mã OTP (Google/Microsoft Authenticator)
Passkey	Chuẩn đăng nhập không mật khẩu bằng sinh trắc học
BitLocker / FileVault	Mã hóa ổ đĩa trên Windows / macOS

Câu hỏi ôn tập (câu 1 – 8)

1. Phân biệt LAN và WAN. Vẽ sơ đồ mạng đơn giản cho một studio dựng phim 5 máy dùng chung NAS, có Wi-Fi cho khách.

2. DNS làm gì? Điều gì xảy ra nếu máy chủ DNS bị lỗi — người học còn vào được web bằng cách nào?

3. Phân tích URL sau, chỉ ra tên miền thật và giải thích tại sao nó đáng ngờ: https://google.com.security-verify.xyz/login

4. Ổ khóa HTTPS có nghĩa là trang web an toàn không? Giải thích.

5. Gói mạng 200 Mbps download / 50 Mbps upload. Tính thời gian lý thuyết để gửi file video 8 GB cho khách hàng. Nêu 2 cách rút ngắn thời gian này.

6. Áp dụng phương pháp SIFT để kiểm chứng một tin “Từ ngày mai, toàn bộ tài khoản mạng xã hội chưa xác thực danh tính sẽ bị khóa vĩnh viễn” lan truyền trên Facebook.

7. Nêu 5 dấu hiệu nhận biết video deepfake. Tại sao các dấu hiệu này ngày càng kém hiệu quả?

8. Phân biệt đồng bộ và sao lưu. Tại sao không nên mở file dự án Premiere trực tiếp từ thư mục Google Drive đang đồng bộ?

Câu hỏi ôn tập (câu 9 – 15)

9 Người học gửi bản dựng cho khách hàng duyệt. Chọn quyền chia sẻ nào? Phạm vi nào? Tại sao?

10 Ransomware là gì? Biện pháp phòng ngừa duy nhất thực sự hiệu quả là gì?

11 Người học nhận email từ “Adobe” báo tài khoản Creative Cloud sắp bị khóa vì lỗi thanh toán, kèm liên kết cập nhật. Liệt kê các bước kiểm tra trước khi hành động.

12 Tại sao “mỗi tài khoản một mật khẩu” quan trọng hơn “mật khẩu có ký tự đặc biệt”? Password manager giải quyết vấn đề gì?

13 So sánh 2FA qua SMS và qua ứng dụng xác thực. Tại sao email chính là tài khoản cần bật 2FA đầu tiên?

14 Người học quay một phim tài liệu có phỏng vấn nhiều người dân. Theo Nghị định 13/2023, người học cần làm gì với hình ảnh và thông tin của họ?

15 Laptop chứa toàn bộ dự án tốt nghiệp bị mất ở quán cà phê. Liệt kê theo thứ tự các việc cần làm trong 1 giờ đầu.

Bài tập tìm hiểu (chọn 2 trong 7)

1 Cáp quang biển

Tuyến cáp của Việt Nam; vì sao cáp đứt mạng chậm; đường đi của dữ liệu khi xem YouTube

2 Một vụ lừa đảo thực tế

Kỹ thuật tâm lý, dấu hiệu bị bỏ qua, bước phát hiện

3 Deepfake trong điện ảnh

2 ví dụ; ứng dụng chính đáng và ranh giới đạo đức; quyền hình ảnh số

4 So sánh dịch vụ đám mây

Nhóm 5 người, 500 GB, 6 tháng: 3 phương án, chi phí, đề xuất

5 Kiểm tra rò rỉ dữ liệu

haveibeenpwned.com: email lộ ở đâu, dữ liệu gì; bài học từ một vụ lớn

6 Nghị định 13/2023 và người sáng tạo

8 quyền của chủ thể dữ liệu; nghĩa vụ khi ghi hình người khác; mẫu giấy đồng ý

7 Passkey

Là gì, khác 2FA ở đâu, dịch vụ hỗ trợ; tạo passkey cho tài khoản Google

GHI NHỚ BA ĐIỀU

1. **Mỗi tài khoản một mật khẩu, dùng trình quản lý mật khẩu**
2. **Bật xác thực hai yếu tố bằng ứng dụng, bắt đầu từ email chính**
3. **Sao lưu 3-2-1, có một bản không kết nối mạng**

Chương tiếp theo: Chương 3. Bản quyền số, an sinh số và công dân số