CHƯƠNG 2
INTERNET, LƯU TRỮ ĐÁM MÂY VÀ AN TOÀN THÔNG TIN

Mục tiêu chương

Sau khi học xong chương này, người học có thể:

- **Giải thích** được cách mạng máy tính và Internet hoạt động: địa chỉ IP, DNS, HTTPS, băng thông, độ trễ; phân biệt được các thiết bị mạng và chuẩn Wi-Fi.
- **Tìm kiếm** thông tin hiệu quả bằng kỹ thuật tìm kiếm nâng cao; đánh giá được độ tin cậy của nguồn; nhận diện được tin giả và nội dung deepfake.
- **Sử dụng** được dịch vụ lưu trữ đám mây để lưu trữ, đồng bộ, chia sẻ và cộng tác trên file dự án; xây dựng quy trình làm việc với file dung lượng lớn.
- **Nhận biết** được các mối đe dọa an ninh mạng phổ biến (mã độc, lừa đảo, tấn công phi kỹ thuật) và áp dụng được các biện pháp bảo vệ thiết bị, tài khoản, dữ liệu cá nhân.
- **Quản lý** được danh tính số của bản thân và hiểu các quy định pháp luật Việt Nam về an ninh mạng và bảo vệ dữ liệu cá nhân.

2.1. Mạng máy tính

2.1.1. Khái niệm và lợi ích

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. Trước khi có mạng, muốn chuyển file từ máy này sang máy khác phải dùng đĩa mềm, USB; muốn in phải nối trực tiếp máy in vào máy tính. Ngày nay, mạng cho phép hàng chục người trong một studio cùng truy cập kho footage trên máy chủ, cùng chỉnh sửa một tài liệu trên Google Docs, gửi bản dựng cho khách hàng ở nước ngoài trong vài phút.

Lợi ích cốt lõi của mạng máy tính: chia sẻ dữ liệu và tài nguyên (máy in, ổ lưu trữ, phần mềm); giao tiếp (email, chat, video call); truy cập thông tin (web); làm việc cộng tác từ xa; và với ngành sáng tạo — phân phối tác phẩm đến khán giả toàn cầu.

2.1.2. Phân loại mạng

Bảng 2.1 — Phân loại mạng theo phạm vi địa lý

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

Theo phương thức kết nối: mạng có dây (cáp Ethernet — ổn định, tốc độ cao 1-10 Gbps, độ trễ thấp, dùng cho máy dựng và NAS) và mạng không dây (Wi-Fi — tiện lợi, tốc độ thấp hơn và dao động, dùng cho laptop, điện thoại). Nguyên tắc: máy làm việc chính với file lớn nên cắm dây; Wi-Fi cho di động.

2.1.3. Thiết bị mạng



Hình 2.1 — Các thiết bị mạng thường gặp: (a) modem băng rộng (ONT cáp quang có hình dạng và chức năng tương tự); (b) router Wi-Fi; (c) switch 8 cổng; (d) access point gắn trần. Ảnh (a): Aravind Sivaraj, CC BY-SA 3.0. Ảnh (b): Evan-Amos, phạm vi công cộng. Ảnh (c): Zuzu, CC BY-SA 3.0. Ảnh (d): Sabbo91, CC BY-SA 4.0. Nguồn: Wikimedia Commons.

- **Modem (ONT — Optical Network Terminal):** Thiết bị nhà mạng (Viettel, VNPT, FPT) cấp, chuyển tín hiệu cáp quang thành tín hiệu mạng. Là "cửa ngõ" nối nhà người học với Internet.
- **Router (bộ định tuyến):** Phân phối kết nối Internet cho nhiều thiết bị, cấp địa chỉ IP nội bộ, có tường lửa cơ bản. Hầu hết router gia đình tích hợp Wi-Fi. Nhà mạng thường cấp thiết bị kết hợp modem + router.
- **Switch (bộ chuyển mạch):** Mở rộng số cổng có dây. Studio có 10 máy dựng cần switch 16-24 cổng Gigabit hoặc 10 Gigabit để truy cập NAS nhanh.
- **Access Point (điểm truy cập):** Phát Wi-Fi mở rộng vùng phủ. Hệ thống Mesh Wi-Fi (nhiều access point phối hợp) cho nhà nhiều tầng, trường quay rộng.
- **Card mạng (NIC):** Trên máy tính, cổng Ethernet (RJ45) hoặc chip Wi-Fi. Laptop mỏng thường bỏ cổng Ethernet — cần adapter USB-C to Ethernet khi làm việc với file lớn.
- **Cáp mạng:** Cat5e (1 Gbps), Cat6 (1-10 Gbps ngắn), Cat6a (10 Gbps). Studio nên đi Cat6a để chuẩn bị cho 10 Gbps.

2.1.4. Wi-Fi

Bảng 2.2 — Các chuẩn Wi-Fi

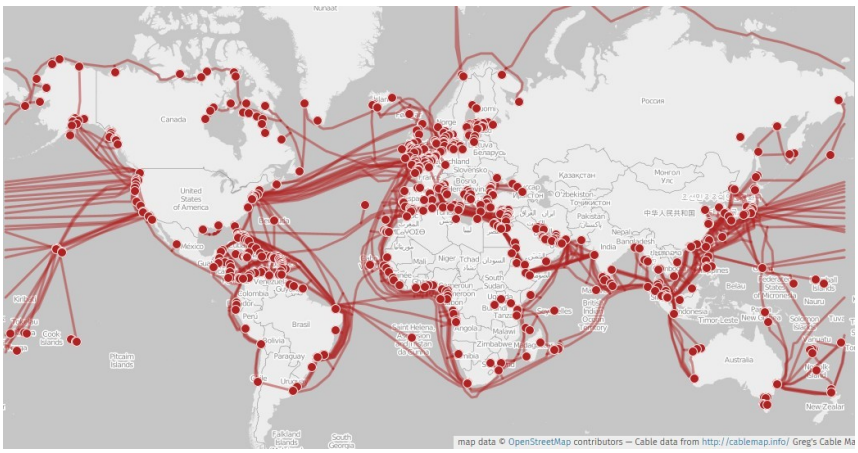
Chuẩn	Tên thương mại	Tốc độ tối đa	Ghi chú
802.11ac	Wi-Fi 5 (2014)	~1-3 Gbps	Phổ biến nhất hiện nay, băng tần 5 GHz
802.11ax	Wi-Fi 6 (2019)	~9,6 Gbps	Tốt hơn khi nhiều thiết bị; Wi-Fi 6E thêm băng 6 GHz
802.11be	Wi-Fi 7 (2024)	~46 Gbps	Mới nhất, độ trễ rất thấp

Băng tần: 2,4 GHz xuyên tường tốt, xa hơn, nhưng chậm và nhiễu (nhiều thiết bị dùng chung); 5 GHz nhanh hơn, ít nhiễu, nhưng tầm ngắn; 6 GHz (Wi-Fi 6E/7) nhanh nhất, tầm ngắn nhất. Khi truyền file lớn, ưu tiên kết nối 5 GHz hoặc cắm dây.

Bảo mật Wi-Fi: WEP (đã lỗi thời, phá được trong vài phút — không bao giờ dùng), WPA2 (an toàn, phổ biến), WPA3 (mới nhất, tốt nhất). 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 vì chủ nhà chưa từng đổi.

2.2. Internet hoạt động như thế nào?

Internet là mạng của các mạng — hàng tỷ thiết bị trên toàn cầu kết nối với nhau qua hệ thống cáp quang xuyên đại dương, vệ tinh, và các trung tâm dữ liệu. Không ai "sở hữu" Internet; nó vận hành nhờ các giao thức (protocol) chung mà mọi thiết bị đều tuân theo.



Hình 2.2 — Bản đồ các tuyến cáp quang biển quốc tế — hạ tầng vật lý của Internet. Dữ liệu cáp: Greg Mahlknecht (cablemap.info), bản đồ nền OpenStreetMap, CC BY-SA 2.0, Wikimedia Commons.

2.2.1. Địa chỉ IP

Mỗi thiết bị trên mạng có một địa chỉ IP (Internet Protocol) duy nhất, như địa chỉ nhà để bưu điện gửi thư. IPv4 có dạng 4 số cách nhau bằng dấu chấm: 192.168.1.15 (khoảng 4,3 tỷ địa chỉ — đã cạn). IPv6 có dạng dài hơn: 2001:0db8:85a3::8a2e:0370:7334 (340 tỷ tỷ tỷ tỷ địa chỉ).

- **IP nội bộ (private):** Router cấp cho thiết bị trong nhà/studio, thường dạng 192.168.x.x hoặc 10.x.x.x. Chỉ có ý nghĩa trong mạng nội bộ.
- **IP công cộng (public):** Nhà mạng cấp cho router của người học, là địa chỉ mà cả Internet nhìn thấy. Tìm bằng cách tìm kiếm "what is my IP". Lưu ý: IP công cộng tiết lộ vị trí đại khái (thành phố) và nhà mạng của người học.
- **IP tĩnh / động:** Hầu hết người dùng có IP động (thay đổi mỗi lần kết nối). Server, NAS cần truy cập từ xa dùng IP tĩnh hoặc dịch vụ DDNS.

2.2.2. DNS — Danh bạ của Internet

Con người nhớ tên (youtube.com), máy tính chỉ hiểu số (142.250.190.14). DNS (Domain Name System) là hệ thống dịch tên miền thành địa chỉ IP. Khi người học gõ youtube.com: máy tính hỏi máy chủ DNS "youtube.com ở đâu?" → DNS trả lời IP → trình duyệt kết nối đến IP đó. Toàn bộ mất vài mili giây.

Cấu trúc tên miền: www.skda.edu.vn gồm: .vn (tên miền quốc gia Việt Nam), .edu (giáo dục), skda (tên tổ chức), www (tên máy chủ). Các đuôi phổ biến: .com (thương mại), .org (tổ chức), .gov (chính phủ), .edu (giáo dục), .vn (Việt Nam).

Máy chủ DNS: Mặc định dùng DNS của nhà mạng. Có thể đổi sang DNS công cộng nhanh và an toàn hơn: 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".

2.2.3. Web, URL, HTTP và HTTPS

World Wide Web (WWW) là một dịch vụ chạy trên Internet (bên cạnh email, FTP, game online...). Web gồm các trang được viết bằng HTML, liên kết với nhau bằng hyperlink, truy cập bằng trình duyệt.

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

Liệt kê 2.1 — Ví dụ một địa chỉ URL đầy đủ

```
https://www.skda.edu.vn/tuyen-sinh/2026/thong-bao.html?lang=vi#muc-2
```

- **https://** — giao thức (protocol)
- **www.skda.edu.vn** — tên miền (domain) — phần *quan trọng nhất* để nhận biết trang web thật/giả
- **/tuyen-sinh/2026/thong-bao.html** — đường dẫn đến trang cụ thể
- **?lang=vi** — tham số truy vấn
- **#muc-2** — vị trí trong trang

HTTP so với HTTPS: HTTP truyền dữ liệu dạng văn bản thuần — ai ở giữa (quán cà phê, nhà mạng, hacker) đều đọc được. HTTPS mã hóa toàn bộ dữ liệu bằng chứng chỉ SSL/TLS — hiển thị biểu tượng ổ khóa trên trình duyệt. Quy tắc: *không bao giờ* nhập mật khẩu, thông tin thẻ trên trang http:// không có ổ khóa. Tuy nhiên, có ổ khóa không có nghĩa là trang web đáng tin — trang lừa đảo cũng có thể dùng HTTPS. Ổ khóa chỉ đảm bảo dữ liệu được mã hóa, không đảm bảo người nhận là ai.

2.2.4. Băng thông, tốc độ và độ trễ

Ba khái niệm hay bị nhầm lẫn nhưng rất quan trọng với người làm việc với file lớn:

- **Băng thông (Bandwidth):** Lượng dữ liệu tối đa truyền được mỗi giây, đo bằng Mbps (megabit/giây) hoặc Gbps. Gói cáp quang gia đình Việt Nam 2026 phổ biến 150 Mbps - 1 Gbps.
- **Tốc độ thực tế (Throughput):** Luôn thấp hơn băng thông do nhiều yếu tố. Kiểm tra bằng speedtest.net hoặc fast.com. Lưu ý phân biệt tốc độ tải xuống (download) và tải lên (upload) — nhiều gói có upload thấp hơn download nhiều, ảnh hưởng trực tiếp đến việc gửi video.
- **Độ trễ (Latency/Ping):** Thời gian tín hiệu đi và về, đo bằng mili giây. Quan trọng với video call, game, điều khiển từ xa. Dưới 50 ms là tốt.

> **Quy đổi cần nhớ: 8 bit = 1 byte**
>
> *Tốc độ mạng đo bằng bit (Mbps), dung lượng file đo bằng byte (MB). Gói 100 Mbps lý thuyết tải 12,5 MB/s; thực tế khoảng 10 MB/s. Gửi file video 5 GB (5.000 MB) với upload 50 Mbps (≈6 MB/s) mất khoảng 14 phút. Với upload 10 Mbps mất hơn 1 giờ. Biết cách tính này giúp người học lập kế hoạch nộp bài, gửi file cho khách hàng.*

2.2.5. Trình duyệt web

Trình duyệt (browser) là phần mềm hiển thị trang web: Google Chrome (~65% thị phần), Microsoft Edge (mặc định trên Windows, nhẹ hơn Chrome), Safari (Apple), Firefox (mã nguồn mở, chú trọng riêng tư), Brave (chặn quảng cáo sẵn). Các tính năng cần biết:

- **Tab và quản lý tab:** Ctrl+T tab mới, Ctrl+W đóng tab, Ctrl+Shift+T mở lại tab vừa đóng, Ctrl+Tab chuyển tab. Nhóm tab (tab groups) để tổ chức theo dự án.
- **Bookmark (Ctrl+D):** Lưu trang hay dùng. Tổ chức bookmark theo thư mục như quản lý file.
- **Lịch sử (Ctrl+H) và Cache:** Trình duyệt lưu lịch sử duyệt và bản sao tạm của trang (cache) để tải nhanh hơn. Xóa bằng Ctrl+Shift+Delete khi máy dùng chung hoặc trang web hiển thị lỗi.
- **Chế độ ẩn danh (Ctrl+Shift+N):** Không lưu lịch sử, cookie trên máy. Nhưng *không* ẩn danh với nhà mạng, trang web, hay cơ quan — chỉ ẩn với người dùng chung máy.
- **Tiện ích mở rộng (Extensions):** uBlock Origin (chặn quảng cáo), Bitwarden (quản lý mật khẩu), Grammarly. Cẩn thận: extension lạ có thể đọc mọi thứ người học gõ.
- **Đồng bộ:** Đăng nhập tài khoản Google/Microsoft để đồng bộ bookmark, mật khẩu, tab giữa các thiết bị.
- **Developer Tools (F12):** Xem mã nguồn trang, kiểm tra tốc độ tải, tải ảnh/video từ trang. Sẽ dùng ở môn Tin học chuyên ngành.

2.2.6. VPN — Mạng riêng ảo

VPN (Virtual Private Network) tạo một "đường hầm" mã hóa giữa thiết bị của người học và máy chủ VPN. Mọi dữ liệu đi qua đường hầm này đều được mã hóa, và trang web đích chỉ thấy địa chỉ IP của máy chủ VPN, không thấy IP thật của người học.

Công dụng chính đáng: (1) Bảo vệ dữ liệu khi dùng Wi-Fi công cộng — quán cà phê, sân bay, khách sạn; (2) Truy cập mạng nội bộ công ty/trường từ xa (VPN doanh nghiệp); (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 — "nếu bạn không trả tiền, bạn là sản phẩm". VPN uy tín: Proton VPN (có gói miễn phí tử tế), Mullvad, NordVPN, ExpressVPN. VPN không giúp người học ẩn danh hoàn toàn và không phải công cụ để vi phạm pháp luật.

2.3. Tìm kiếm và đánh giá thông tin

Người học không chỉ cần tìm được thông tin mà còn phải đánh giá được độ tin cậy, tính chính xác của thông tin đó. Trong thời đại AI tạo sinh và tin giả lan tràn, đây là kỹ năng sống còn — đặc biệt với người làm truyền thông, báo chí, nội dung số.

2.3.1. Kỹ thuật tìm kiếm nâng cao

Google (và Bing, DuckDuckGo) hỗ trợ các toán tử giúp thu hẹp kết quả chính xác:

Bảng 2.3 — Các 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:	Định nghĩa	define:compositing
related:	Trang tương tự	related:artgrid.io

Mẹo tìm kiếm cho ngành sáng tạo: tìm tài nguyên miễn phí có bản quyền rõ ràng ("royalty free" "CC0" "public domain"); tìm bằng tiếng Anh để có kết quả phong phú hơn; dùng Google Images > Tools > Usage rights > Creative Commons licenses; tìm ngược bằng hình ảnh (Google Lens, TinEye) để tìm nguồn gốc ảnh hoặc kiểm tra ảnh có bị chỉnh sửa.

2.3.2. Tìm kiếm với AI

Từ 2023, các công cụ AI (ChatGPT, Claude, Gemini, Perplexity, Copilot) trở thành cách tìm kiếm phổ biến. Chúng tổng hợp thông tin nhanh, trả lời trực tiếp thay vì đưa danh sách liên kết. Tuy nhiên, AI có thể "ảo giác" (hallucination) — bịa ra thông tin, trích dẫn, số liệu nghe rất thuyết phục nhưng sai hoàn toàn. Nguyên tắc: dùng AI để định hướng, tóm tắt, gợi ý từ khóa; nhưng luôn kiểm chứng thông tin quan trọng bằng nguồn gốc. Chủ đề này sẽ học sâu ở Chương 9.

2.3.3. Đánh giá độ tin cậy nguồn thông tin

Phương pháp SIFT (Mike Caulfield, 2019) — bốn bước nhanh để kiểm tra bất kỳ thông tin nào trên mạng:

- **S — Stop (Dừng lại):** Trước khi tin hoặc chia sẻ, dừng lại. Cảm xúc mạnh (phẫn nộ, sợ hãi, quá vui) là dấu hiệu cần cảnh giác — tin giả được thiết kế để kích động cảm xúc.

- **I — Investigate the source (Điều tra nguồn):** Ai đăng? Trang web/tài khoản này là gì? Tìm kiếm tên nguồn trên Wikipedia hoặc Google để biết uy tín. Tài khoản mới lập, ít người theo dõi, không có thông tin xác thực → nghi ngờ.
- **F — Find better coverage (Tìm nguồn khác):** Các báo lớn, cơ quan chính thức có đưa tin này không? Nếu một "tin chấn động" chỉ có một nguồn duy nhất → rất có thể là giả.
- **T — Trace to the original (Truy về gốc):** Ảnh, video, trích dẫn thường bị cắt xén, lấy khỏi ngữ cảnh. Tìm bản gốc đầy đủ.

Tiêu chí bổ sung khi đánh giá tài liệu học thuật (CRAAP): Currency (thời điểm — thông tin có còn cập nhật?), Relevance (liên quan), Authority (thẩm quyền — tác giả có chuyên môn?), Accuracy (chính xác — có dẫn chứng, có bị phản bác?), Purpose (mục đích — thông tin, bán hàng, tuyên truyền?).

Bảng 2.4 — Các mức độ tin cậy của nguồn thông tin

Mức tin cậy	Loại nguồn	Ví dụ
Cao	Cơ quan chính phủ, tổ chức quốc tế, tạp chí khoa học có bình duyệt, sách giáo trình, tài liệu chính thức của nhà sản xuất	moet.gov.vn, unesco.org, tài liệu hướng dẫn Adobe/Blackmagic, Wikipedia (kiểm tra nguồn trích dẫn)
Trung bình	Báo chí chính thống, chuyên gia có tên tuổi, diễn đàn chuyên ngành uy tín	VnExpress, Tuổi Trẻ, No Film School, Creative COW, Stack Exchange
Thấp	Blog cá nhân, mạng xã hội, trang tổng hợp, video YouTube 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 do AI tạo không kiểm chứng	Trang có tên gần giống báo lớn (vnexpres.com), nhóm chat lan truyền

2.3.4. Tin giả và Deepfake

Tin giả (fake news, misinformation, disinformation) là thông tin sai lệch được lan truyền vô tình (misinformation) hoặc cố ý để lừa dối, thao túng (disinformation). Dấu hiệu nhận biết: tiêu đề giật gân viết hoa, nhiều dấu chấm than; kêu gọi "chia sẻ ngay"; không có tác giả, ngày tháng, nguồn; ảnh không liên quan hoặc đã qua chỉnh sửa; tên miền lạ; lỗi chính tả nhiều; nội dung chỉ xuất hiện trên mạng xã hội.

Deepfake là nội dung (video, ảnh, giọng nói) được AI tạo ra hoặc chỉnh sửa để trông như thật: ghép mặt người này vào thân người khác, tạo video một người nói những điều họ chưa từng nói, nhân bản giọng nói từ vài giây mẫu. Công nghệ này có ứng dụng chính đáng trong điện ảnh (trẻ hóa diễn viên, lồng tiếng đa ngôn ngữ) nhưng cũng bị lạm dụng để lừa đảo (giả giọng người thân gọi

điện vay tiền, giả video lãnh đạo doanh nghiệp yêu cầu chuyển khoản), tống tiền, bôi nhọ.

Dấu hiệu nhận biết deepfake (đang ngày càng khó): chuyển động môi không khớp âm thanh; chớp mắt bất thường (quá ít hoặc quá đều); viền mặt, tóc, tai mờ nhòe hoặc lệch khi quay đầu; ánh sáng trên mặt không khớp với nền; giọng nói thiếu ngữ điệu tự nhiên, không có tiếng thở; bàn tay, ngón tay biến dạng (AI vẫn khó vẽ tay); bối cảnh mờ ảo hoặc chữ trong ảnh vô nghĩa.

Cách xác minh: tìm kiếm ngược hình ảnh/khung hình video (Google Lens, TinEye); kiểm tra nguồn gốc — video có xuất hiện trên kênh chính thức không; dùng công cụ phát hiện (Deepware Scanner, Microsoft Video Authenticator, Intel FakeCatcher); quan trọng nhất — gọi điện xác minh trực tiếp khi có yêu cầu liên quan đến tiền bạc, dù người gọi giống hệt người thân.

> **Người học SKĐA và deepfake**
>
> *Là người sẽ làm việc với công nghệ tạo hình ảnh, người học có trách nhiệm kép: (1) hiểu công nghệ để dùng đúng mục đích sáng tạo và (2) không tạo, không lan truyền nội dung deepfake gây hại. Luật An ninh mạng 2018 và Bộ luật Hình sự có quy định xử phạt hành vi giả mạo hình ảnh, giọng nói người khác để lừa đảo, xúc phạm danh dự. Chương 3 sẽ bàn sâu về đạo đức và pháp lý.*

2.4. Lưu trữ đám mây

2.4.1. Khái niệm

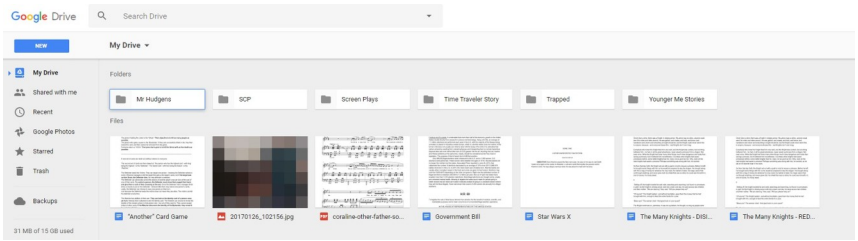
Điện toán đám mây (cloud computing) là mô hình cung cấp tài nguyên máy tính (lưu trữ, xử lý, phần mềm) qua Internet theo nhu cầu. "Đám mây" thực chất là hàng nghìn máy chủ trong các trung tâm dữ liệu khổng lồ của Google, Microsoft, Amazon, Apple đặt khắp thế giới. Khi người học lưu file lên Google Drive, file được sao chép vào nhiều máy chủ ở nhiều địa điểm — nên gần như không bao giờ mất.

Lưu trữ đám mây (cloud storage) là dịch vụ phổ biến nhất: người học tải file lên, truy cập từ bất kỳ thiết bị nào có Internet, chia sẻ cho người khác bằng một đường liên kết. Với ngành sáng tạo, đám mây thay đổi cách làm việc: đạo diễn ở Hà Nội duyệt bản dựng của editor ở TP.HCM, nhóm 5 người cùng viết kịch bản trên một tài liệu, khách hàng nhận file 20 GB không cần gặp mặt.

2.4.2. Các dịch vụ phổ biến

Bảng 2.5 — Các dịch vụ lưu trữ đám mây phổ biến

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 cộng tác thời gian thực; phổ biến nhất ở Việt Nam; tài khoản trường (.edu) thường có dung lượng lớn
Microsoft OneDrive	5 GB	100 GB ~45.000đ; 1 TB kèm Microsoft 365	Tích hợp sâu Windows và Office; Files On-Demand tiết kiệm ổ cứng; tài khoản trường có 1 TB+
Dropbox	2 GB	2 TB ~12 USD/tháng	Đồng bộ nhanh và tin cậy nhất; Dropbox Replay để duyệt video; phổ biến trong studio quốc tế
iCloud Drive	5 GB	50 GB ~25.000đ; 2 TB ~250.000đ	Tích hợp hệ sinh thái Apple; tự động sao lưu iPhone, ảnh
Frame.io (Adobe)	2 GB	Kèm Creative Cloud	Chuyên duyệt video: comment theo timecode, so sánh phiên bản, tích hợp Premiere/Resolve
WeTransfer / Smash	2 GB/lần (WeTransfer), không giới hạn (Smash)	WeTransfer Pro ~10 USD	Gửi file lớn một lần, liên kết hết hạn sau 7 ngày, không cần tài khoản người nhận



Hình 2.3 — Giao diện web của Google Drive, mục My Drive: thanh bên trái có My Drive, Shared with me, Recent, Starred, Trash và dung lượng đã dùng; phần giữa là các thư mục và tệp. Ảnh minh họa giao diện phiên bản năm 2017, giao diện hiện nay đổi màu sắc nhưng bố cục tương tự. Ảnh: Hazumane, CC BY-SA 4.0, Wikimedia Commons (đã chỉnh sửa).

2.4.3. Đồng bộ và sao lưu — Hai khái niệm khác nhau

Đồng bộ (Sync): Thư mục trên máy và trên đám mây luôn giống nhau. Sửa ở đâu, nơi kia cũng thay đổi. Xóa ở máy → xóa trên đám mây. Tiện cho làm việc nhiều thiết bị, nhưng *không phải* backup — nếu người học xóa nhầm hoặc bị ransomware mã hóa file, bản trên đám mây cũng bị theo (dù hầu hết dịch vụ giữ lịch sử phiên bản 30 ngày để khôi phục).

Sao lưu (Backup): Sao chép một chiều từ máy lên nơi lưu trữ, giữ nhiều phiên bản theo thời gian. Xóa ở máy không ảnh hưởng bản backup. Google Drive Desktop có chế độ "Backup" cho thư mục; OneDrive có "PC folder backup"; hoặc dùng dịch vụ chuyên backup (Backblaze — không giới hạn dung lượng ~9 USD/tháng).

Với quy tắc 3-2-1 đã học: đám mây đóng vai trò bản sao "ở nơi khác". Nhưng để đúng nghĩa backup, hãy dùng chế độ backup hoặc giữ thêm một bản trên ổ cứng ngoài không đồng bộ.

2.4.4. Ứng dụng đồng bộ trên máy tính

Cài Google Drive Desktop hoặc OneDrive (có sẵn trên Windows) để đám mây xuất hiện như một ổ đĩa trong File Explorer. Hai chế độ:

- **Stream / Files On-Demand:** File hiện trong File Explorer nhưng chỉ tải về khi mở. Tiết kiệm ổ cứng — phù 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, có thể làm việc offline. Cần ổ cứng đủ lớn.

Lưu ý quan trọng cho ngành sáng tạo: *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 ổ SSD nội bộ, sao chép hoặc backup lên đám mây theo lịch.

2.4.5. Chia sẻ và phân quyền

Khi chia sẻ file/thư mục trên Google Drive hoặc OneDrive, người học kiểm soát ai được làm gì:

Bảng 2.6 — Các quyền chia sẻ file và thư mục

Quyền	Người nhận có thể	Dùng khi
Viewer (Xem)	Xem, tải về (có thể tắt tải)	Gửi bản dựng cho khách duyệt, nộp bài cho giảng viên
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

Phạm vi chia sẻ: (1) Restricted — chỉ người được thêm email; (2) Anyone with the link — ai có liên kết đều truy cập được (tiện nhưng liên kết có thể bị

chuyển tiếp ngoài ý muốn); (3) Trong tổ chức — chỉ tài khoản cùng trường/công ty. Nguyên tắc: dữ liệu nhạy cảm (kịch bản chưa công bố, footage khách hàng, thông tin cá nhân) chỉ chia sẻ Restricted và đặt ngày hết hạn.

Kiểm tra định kỳ: Google Drive > "Shared with me" và "Shared by me" để xem người học đang chia sẻ gì với ai, thu hồi quyền khi dự án kết thúc.

2.4.6. Quy trình làm việc với file lớn

Dự án video, ảnh RAW, 3D có dung lượng hàng chục đến hàng trăm GB — không thể upload/download toàn bộ mỗi lần. Quy trình chuyên nghiệp:

1. Footage gốc lưu trên SSD nội bộ + ổ ngoài (không đưa lên đám mây trừ khi có gói dung lượng lớn).
2. Tạo proxy — bản video độ phân giải thấp (720p, dung lượng bằng 1/10) — để dựng và chia sẻ. Premiere, DaVinci đều có chức năng tạo proxy tự động.
3. File dự án (.prproj, .drp — chỉ vài MB) và tài liệu đưa lên đám mây, đồng bộ nhóm.
4. Bản duyệt (review) xuất H.264 1080p dung lượng nhỏ, gửi qua Frame.io, Google Drive, hoặc YouTube unlisted.
5. Bản cuối (final) chất lượng cao gửi qua WeTransfer/Smash, hoặc giao trực tiếp bằng ổ cứng nếu quá lớn.
6. Kết thúc dự án: archive toàn bộ vào ổ cứng ngoài + cloud archive (Google One 2 TB, Backblaze B2 giá rẻ theo GB).

2.5. Giao tiếp trực tuyến

2.5.1. Email chuyên nghiệp

Email vẫn là kênh giao tiếp chính thức trong học tập và công việc: nộp bài, liên hệ giảng viên, ứng tuyển, làm việc với khách hàng. Nguyên tắc viết email chuyên nghiệp:

- **Địa chỉ email nghiêm túc:** nguyenvana@gmail.com hoặc email trường, không phải cobebutchi2005@... Dùng email trường (.edu.vn) 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 (em là… lớp…) → Nội dung chính (ngắn gọn, đánh số nếu nhiều ý) → Lời cảm ơn → Chữ ký (họ tên, lớp, số điện thoại).
- **File đính kèm:** Đặt tên đúng quy ước; file lớn (>25 MB) gửi liên kết Drive thay vì đính kèm; nói rõ trong nội dung có đính kèm gì.
- **Cc / Bcc:** Cc để người khác biết; Bcc khi gửi nhiều người mà không muốn lộ email của nhau (ví dụ gửi thông báo cho cả lớp).
- **Trả lời trong 24 giờ;** dùng Reply All cẩn thận; đọc lại trước khi gửi; không viết email khi đang tức giận.

2.5.2. Các nền tảng giao tiếp và họp trực tuyến

Bảng 2.7 — Các 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 trong nước, 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 với Google Workspace
Zoom	Ổn định, nhiều tính năng (breakout room, ghi hình)	Hội thảo, lớp học đông
Slack / Discord	Kênh chủ đề, tích hợp công cụ, cộng đồng	Nhóm sản xuất, cộng đồng sáng tạo quốc tế
Telegram	Nhanh, gửi file 2 GB, bot, kênh	Cộng đồng, chia sẻ tài nguyên

Nghi thức họp trực tuyến: kiểm tra mic, camera, mạng trước 5 phút; tắt mic khi không nói; bật camera khi có thể (thể hiện sự tôn trọng); đặt tên hiển thị đúng (Họ tên — Lớp); nền gọn gàng hoặc dùng nền ảo; không làm việc khác trong khi họp; ghi chú và tóm tắt sau họp. Chi tiết về quy tắc ứng xử số (netiquette) và danh tính số sẽ học ở Chương 3.

2.6. An toàn thông tin

An toàn thông tin (information security) là bảo vệ dữ liệu và hệ thống khỏi truy cập trái phép, phá hoại, đánh cắp. Với người học ngành sáng tạo, tài sản cần bảo vệ gồm: tài khoản (email, mạng xã hội, ngân hàng, Adobe, Google Drive), dữ liệu (dự án, portfolio, footage khách hàng), thiết bị (laptop, điện thoại, ổ cứng), và danh tính số (hình ảnh, uy tín trên mạng).

Việt Nam năm 2025 ghi nhận thiệt hại do lừa đảo trực tuyến ước tính hàng nghìn tỷ đồng; 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. Hiểu các mối đe dọa là bước đầu tiên để phòng tránh.

2.6.1. Các mối đe dọa phổ biến

a) Mã độc (Malware)

Bảng 2.8 — Các loại mã độc phổ biến

Loại	Hoạt động	Lây qua
Virus	Gắn vào file/chương trình, lây lan khi chạy, phá hoại dữ liệu	File tải về, USB, email đính kèm
Trojan	Giả dạng phần mềm hữu ích (crack, tool), bên trong chứa mã độc mở cửa hậu	Phần mềm crack, "tool hack", trò chơi sao chép trái phép
Ransomware	Mã hóa toàn bộ file, đòi tiền chuộc (Bitcoin) để giải mã	Email phishing, phần mềm crack, lỗ hổng chưa vá
Spyware / Keylogger	Theo dõi, ghi lại mọi phím gõ, chụp màn hình, đánh cắp mật khẩu	Extension trình duyệt 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 người học đào tiền ảo — máy chậm, nóng, tốn điện	Phần mềm crack, trang web độc

Ransomware là mối đe dọa nghiêm trọng nhất với người làm sáng tạo: một buổi sáng, toàn bộ dự án 3 tháng bị mã hóa, màn hình hiện thông báo đòi 500 USD Bitcoin. Không có backup = mất trắng. Trả tiền cũng không chắc lấy lại được. Phòng ngừa duy nhất: backup 3-2-1 với ít nhất một bản không kết nối mạng (ổ cứng ngoài rút ra sau khi sao lưu).

b) Lừa đảo (Phishing) và tấn công phi kỹ thuật (Social Engineering)

Phishing là lừa người dùng tự nộp thông tin (mật khẩu, mã OTP, số thẻ) bằng cách giả mạo tổ chức uy tín. Không cần hack hệ thống — chỉ cần lừa được con người. Các hình thức:

- **Email phishing:** "Tài khoản Google của bạn sắp bị khóa, nhấn vào đây để xác minh" → liên kết dẫn đến trang đăng nhập giả giống hệt Google, người học nhập mật khẩu → mất tài khoản.
- **Smishing (SMS):** "Bạn có bưu phẩm chưa nhận, truy cập link để xem" — tin nhắn giả danh bưu điện, ngân hàng, cơ quan thuế.
- **Vishing (gọi điện):** Giả danh công an ("bạn liên quan đến vụ rửa tiền"), nhân viên ngân hàng, giáo viên ("con bạn bị tai nạn"), kèm deepfake giọng nói. Tạo hoảng sợ để nạn nhân chuyển tiền ngay.
- **Lừa đảo việc làm:** "Cộng tác viên chốt đơn Shopee", "Like video TikTok nhận tiền" — ban đầu trả tiền thật để tạo tin tưởng, sau đó yêu cầu nạp tiền để "nhận nhiệm vụ lớn".

- **Lừa đảo tình cảm, đầu tư:** Làm quen qua mạng, xây dựng tình cảm, rồi rủ đầu tư tiền ảo, forex trên sàn giả.
- **Giả mạo trong ngành sáng tạo:** "Nhãn hàng X muốn hợp tác, gửi portfolio và CCCD để ký hợp đồng"; "Casting phim lớn, đóng phí hồ sơ"; email giả từ "Adobe" yêu cầu cập nhật thanh toán.

> **Dấu hiệu nhận biết phishing**
>
> *Tạo khẩn cấp, sợ hãi ("trong 24 giờ", "ngay lập tức") · Địa chỉ người gửi lạ hoặc gần giống thật (support@g00gle.com, adobe-billing@gmail.com) · Liên kết hiển thị khác liên kết thật (rê chuột lên liên kết để xem trước khi nhấn) · Lỗi chính tả, ngữ pháp, xưng hô chung chung ("Kính gửi khách hàng") · Yêu cầu mật khẩu, OTP, thông tin thẻ — tổ chức thật không bao giờ hỏi những thứ này qua email/điện thoại · Đính kèm file .exe, .zip, .docm bất ngờ · Quá tốt để là thật (trúng thưởng, việc nhẹ lương cao)*

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

c) Các mối đe dọa khác

- **Tấn công dò mật khẩu (Brute force / Credential stuffing):** Dùng máy thử hàng triệu mật khẩu; hoặc dùng mật khẩu bị lộ từ trang A để thử đăng nhập trang B (vì nhiều người dùng chung mật khẩu). Kiểm tra email của người học có trong vụ rò rỉ nào chưa tại haveibeenpwned.com.
- **Wi-Fi giả (Evil twin):** Hacker tạo Wi-Fi tên giống quán cà phê ("Highlands Free"), người học kết nối → mọi dữ liệu không mã hóa bị đọc.
- **Chiếm tài khoản mạng xã hội:** Facebook bị hack → kẻ xấu nhắn tin bạn bè vay tiền. Rất phổ biến ở Việt Nam.
- **Lộ dữ liệu từ dịch vụ:** Trang web người học đăng ký bị hack, lộ email + mật khẩu của hàng triệu người.

2.6.2. Mật khẩu mạnh và trình quản lý mật khẩu

Mật khẩu là lớp bảo vệ đầu tiên và bị xem nhẹ nhất. Máy tính hiện đại thử được hàng tỷ mật khẩu mỗi giây: mật khẩu 8 ký tự chỉ chữ thường bị phá trong vài giây; "123456", "password", "matkhau" bị thử đầu tiên.

Bảng 2.9 — So sánh độ mạnh của mật khẩu

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 không 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 mật khẩu mạnh: (1) Dài — ít nhất 12 ký tự, tốt nhất 16+; độ dài quan trọng hơn độ phức tạp; (2) Dùng cụm từ (passphrase) dễ nhớ với người học nhưng vô nghĩa với người khác; (3) Không chứa thông tin cá nhân (tên, ngày sinh, tên thú cưng, số điện thoại); (4) *mỗi tài khoản một mật khẩu khác nhau* — quan trọng nhất; (5) Không viết ra giấy dán màn hình, không lưu trong file text "matkhau.txt".

Trình quản lý mật khẩu (Password Manager): Người học không thể nhớ 50 mật khẩu khác nhau, mạnh — và không cần. Password manager 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). Các lựa chọn: Bitwarden (miễn phí, mã nguồn mở — khuyến nghị), 1Password, Proton Pass; trình quản lý tích hợp Google Password Manager, iCloud Keychain (tiện nhưng gắn với một hệ sinh thái).

2.6.3. Xác thực hai yếu tố (2FA)

Xác thực hai yếu tố (Two-Factor Authentication, 2FA) hay xác thực đa yếu tố (MFA) yêu cầu thêm một bằng chứng ngoài mật khẩu để đăng nhập: thứ người dùng biết (mật khẩu) + thứ người dùng có (điện thoại, khóa vật lý) hoặc thứ người dùng là (vân tay, khuôn mặt). Kể cả khi mật khẩu bị lộ, kẻ xấu vẫn không vào được.

Bảng 2.10 — Các phương thức xác thực hai yếu tố

Phương thức	Độ an toàn	Tiện lợi	Ghi chú
SMS OTP	Thấp	Cao	Bị chiếm SIM (SIM swap), bị lừa đọc OTP. Tốt hơn không có
Ứng dụng xác thực	Cao	Cao	Google Authenticator, Microsoft Authenticator, Authy — mã 6 số đổi mỗi 30 giây, không cần mạng. *khuyến nghị*
Thông báo đẩy	Cao	Rất cao	Gmail hỏi "Có phải bạn đang đăng nhập?" trên điện thoại. Cẩn thận "MFA fatigue" — kẻ xấu spam thông báo đến khi người học bấm nhầm
Khóa vật lý (FIDO2)	Rất cao	Trung bình	YubiKey, Google Titan — chống phishing tuyệt đối. Cho tài khoản quan trọng nhất
Passkey	Rất cao	Rất cao	Chuẩn mới (2023+), thay thế mật khẩu bằng sinh trắc học trên thiết bị. Google, Apple, Microsoft đều hỗ trợ

Bật 2FA ngay cho: email chính (quan trọng nhất — mất email = mất mọi tài khoản dùng email đó để khôi phục), ngân hàng, Facebook/Instagram/TikTok (kênh portfolio và thu nhập của người sáng tạo), Google Drive/iCloud (kho dữ liệu), Adobe/Steam (tài sản số). Lưu mã dự phòng (backup codes) ở nơi an toàn phòng khi mất điện thoại.

2.6.4. Bảo vệ thiết bị

- **Cập nhật hệ điều hành và phần mềm:** Bản vá bảo mật đóng các lỗ hổng mà mã độc khai thác. Ransomware WannaCry (2017) lây nhiễm 200.000 máy tính ở 150 nước chỉ vì họ không cài bản vá Windows đã phát hành 2 tháng trước. Bật cập nhật tự động.
- **Phần mềm chống virus:** Windows Security (Microsoft Defender) tích hợp sẵn, miễn phí, đủ tốt cho hầu hết người dùng — đừng tắt. Phần mềm thứ ba (Kaspersky, Bitdefender, ESET) thêm tính năng. Chỉ cài *một* phần mềm chống virus. macOS có XProtect tích hợp; vẫn nên cẩn thận.
- **Tường lửa (Firewall):** Chặn kết nối mạng trái phép vào/ra máy. Windows Firewall bật mặc định — giữ nguyên.
- **Mã hóa ổ đĩa:** Laptop bị mất/trộm → kẻ xấu tháo ổ cứng đọc toàn bộ dữ liệu, trừ khi đã mã hóa. Windows: BitLocker (bản Pro) hoặc Device Encryption (bản Home, Settings > Privacy & security); macOS: FileVault. Bật ngay cho laptop.

- **Khóa màn hình:** Đặt mật khẩu/PIN/vân tay đăng nhập; tự khóa sau 5 phút không dùng; nhấn Win + L mỗi khi rời máy — kể cả 1 phút. Điện thoại: mã 6 số trở lên hoặc sinh trắc học, không dùng mẫu vẽ đơn giản.
- **Tải phần mềm từ nguồn chính thức:** Trang web nhà sản xuất, Microsoft Store, App Store. Không tải từ trang "download miễn phí", không dùng crack — 90% crack chứa mã độc.
- **USB và ổ ngoài lạ:** Không cắm USB nhặt được hoặc không rõ nguồn. Quét virus USB trước khi mở. Tắt AutoPlay.
- **Tìm thiết bị và xóa từ xa:** Bật Find My Device (Windows), Find My (Apple), Find My Device (Android) — định vị, khóa, xóa dữ liệu khi mất máy.

2.6.5. Bảo vệ dữ liệu cá nhân và quyền riêng tư

Dữ liệu cá nhân là mọi thông tin xác định được người học: họ tên, ngày sinh, CCCD, số điện thoại, email, địa chỉ, ảnh khuôn mặt, giọng nói, vị trí, lịch sử duyệt web, sở thích, và cả tác phẩm sáng tạo mang dấu ấn cá nhân. Trong nền kinh tế số, dữ liệu cá nhân là tài sản có giá — được thu thập, mua bán, dùng để nhắm quảng cáo, thao túng, và lừa đảo.

a) Nguyên tắc chia sẻ tối thiểu

- Trước khi điền form, đăng ký ứng dụng, hỏi: Họ có thực sự cần thông tin này không? Cửa hàng bán áo không cần biết ngày sinh và CCCD của người học.
- Không đăng ảnh CCCD, thẻ người học, vé máy bay, hóa đơn có mã QR lên mạng — kể cả story 24 giờ.
- Không chia sẻ vị trí thời gian thực công khai; tắt định vị trong ảnh (EXIF) khi đăng ảnh.
- Cẩn thận với các "trò chơi" trên Facebook ("Tên ngôi sao của bạn là tên đường + tên thú cưng") — đó chính là câu hỏi bảo mật.
- Dùng email phụ (alias) cho các đăng ký không quan trọng; Gmail cho phép thêm +tag: tuan+shopee@gmail.com.

b) Kiểm soát cài đặt riêng tư

- **Mạng xã hội:** Đặt bài viết mặc định "Bạn bè"; kiểm tra ai xem được danh sách bạn bè, ngày sinh, số điện thoại; tắt nhận diện khuôn mặt; xem lại "Apps and Websites" đã cấp quyền và thu hồi.
- **Điện thoại:** Xem lại quyền từng ứng dụng (Settings > Privacy): ứng dụng đèn pin không cần vị trí và danh bạ. Từ chối quyền không cần thiết.
- **Google/Apple:** myaccount.google.com > Data & privacy: xem và xóa lịch sử vị trí, hoạt động web, YouTube; tắt cá nhân hóa quảng cáo.
- **Trình duyệt:** Chặn cookie bên thứ ba; dùng uBlock Origin; cân nhắc Firefox/Brave cho riêng tư tốt hơn.

c) Danh tính số và dấu chân số

Danh tính số (digital identity) là hình ảnh của người học trên không gian mạng — tổng hợp từ mọi thứ người học đăng, bình luận, thích, và cả những gì người khác đăng về người học. Dấu chân số (digital footprint) gần như không xóa được: ảnh chụp màn hình, Wayback Machine lưu trữ trang web, dữ liệu bị rò rỉ.

Với người làm sáng tạo, danh tính số chính là thương hiệu cá nhân. Nhà tuyển dụng, khách hàng, ban tuyển sinh sau đại học đều tìm kiếm tên người học trên Google trước khi quyết định. Hãy tự tìm tên mình (kèm dấu ngoặc kép) trên Google, Facebook, TikTok định kỳ để biết người khác thấy gì. Tách biệt tài khoản công việc (portfolio, chuyên nghiệp) và cá nhân (bạn bè, riêng tư). Nội dung sẽ bàn sâu ở Chương 3.

2.6.6. An toàn trên mạng Wi-Fi công cộng

- Ưu tiên dùng 4G/5G cá nhân thay vì Wi-Fi công cộng cho giao dịch quan trọng.
- Nếu phải dùng: xác nhận tên Wi-Fi chính xác với nhân viên; chỉ truy cập trang HTTPS; bật VPN; tắt chia sẻ file (Windows: đặt mạng là Public); không đăng nhập ngân hàng, không nhập thẻ.
- Tắt Wi-Fi và Bluetooth khi không dùng; tắt tự động kết nối Wi-Fi mở.

2.6.7. Khi sự cố xảy ra

Bảng 2.11 — Cách xử lý khi sự cố xảy ra

Tình huống	Hành động ngay
Nghi ngờ đã nhấn liên kết phishing, nhập mật khẩu	Đổi mật khẩu *ngay* từ thiết bị khác → bật 2FA nếu chưa → kiểm tra hoạt động đăng nhập lạ (Google: myaccount.google.com/security) → đăng xuất mọi thiết bị → đổi mật khẩu các tài khoản dùng chung mật khẩu
Tài khoản Facebook/Gmail bị chiếm	Dùng chức năng khôi phục (facebook.com/hacked; Google account recovery) → báo bạn bè, người thân đừng chuyển tiền → sau khi lấy lại: đổi mật khẩu, bật 2FA, xem lại ứng dụng đã cấp quyền
Máy nhiễm mã độc / ransomware	Ngắt mạng ngay (rút cáp, tắt Wi-Fi) → không trả tiền chuộc → quét toàn bộ bằng Windows Security hoặc Malwarebytes → khôi phục từ backup → nếu nghiêm trọng: cài lại Windows
Mất laptop/điện thoại	Find My Device: khóa và 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 ngay yêu cầu phong tỏa giao dịch → giữ mọi bằng chứng (tin nhắn, số tài khoản, cuộc gọi) → trình báo công an phường hoặc qua canhbaolua.vn / Cổng cảnh báo an toàn thông tin (chongluadao.vn)
Bị lộ ảnh/thông tin nhạy cảm	Không hoảng, không trả tiền tống tiền → chụp lại bằng chứng → báo cáo nền tảng gỡ nội dung → trình báo công an → tìm hỗ trợ từ người thân, trường, đường dây nóng

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

- **Luật An ninh mạng 2018 (có hiệu lực 01/01/2019):** Quy định các hành vi bị cấm trên không gian mạng: đăng tin sai sự thật gây hoang mang, xúc phạm danh dự người khác, 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 về bảo vệ dữ liệu cá nhân (hiệu lực 01/07/2023):** Văn bản đầu tiên của Việt Nam quy định toàn diện về dữ liệu cá nhân. Chủ thể dữ liệu (người học) có quyền: được biết, đồng ý, truy cập, rút lại sự đồng ý, xóa dữ liệu, hạn chế xử lý, phản đối, khiếu nại, bồi thường. Tổ chức thu thập dữ liệu phải xin phép rõ ràng, chỉ dùng đúng mục đích, bảo mật, và thông báo khi bị rò rỉ.

- **Luật Bảo vệ dữ liệu cá nhân 2025 (Quốc hội thông qua tháng 6/2025, hiệu lực 01/01/2026):** Nâng Nghị định 13 lên thành luật, tăng mức xử phạt, quy định rõ trách nhiệm khi dùng AI xử lý dữ liệu cá nhân.
- **Nghị định 15/2020/NĐ-CP (sửa đổi bởi 14/2022):** Xử phạt hành chính 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), Điều 288 (đưa hoặc sử dụng trái phép thông tin mạng máy tính), Điều 289 (xâm nhập trái phép mạng máy tính), Điều 290 (sử dụng mạng máy tính chiếm đoạt tài sản) — mức phạt tù đến 20 năm.

Ý nghĩa với người học sáng tạo

Khi người học quay phim, chụp ảnh người khác và đăng lên mạng, người học đang xử lý dữ liệu cá nhân của họ (hình ảnh, giọng nói) — cần sự đồng ý, đặc biệt với mục đích thương mại. Khi người học thu thập thông tin khán giả, khách hàng (email, số điện thoại) cho dự án, người học có trách nhiệm bảo mật theo Nghị định 13. Khi người học dùng AI tạo hình ảnh giống người thật, người học có thể vi phạm quyền hình ảnh (Điều 32 Bộ luật Dân sự). Hiểu luật không chỉ để tránh vi phạm, mà còn để bảo vệ chính tác phẩm và dữ liệu của mình.

Tóm tắt chương

- Mạng máy tính chia theo phạm vi (PAN, LAN, WAN); Internet là mạng của các mạng. Thiết bị: modem, router, switch, access point. Máy làm việc file lớn nên cắm dây; Wi-Fi dùng WPA2/WPA3.
- Mỗi thiết bị có địa chỉ IP; DNS dịch tên miền thành IP. URL gồm giao thức, tên miền (quan trọng nhất để nhận biết thật/giả), đường dẫn. HTTPS mã hóa dữ liệu nhưng không đảm bảo trang web đáng tin.
- Băng thông (Mbps) ≠ dung lượng (MB): chia 8. Upload thường thấp hơn download — ảnh hưởng gửi video. VPN bảo vệ trên Wi-Fi công cộng; tránh VPN miễn phí.
- Tìm kiếm nâng cao với toán tử ("", -, site:, filetype:). Đánh giá nguồn bằng SIFT: Stop, Investigate, Find, Trace. AI có thể ảo giác — luôn kiểm chứng.
- Deepfake ngày càng khó nhận biết; xác minh bằng tìm kiếm ngược, kiểm tra nguồn, và gọi điện trực tiếp khi liên quan đến tiền.
- Đám mây: Google Drive, OneDrive, Dropbox, Frame.io. Đồng bộ ≠ backup. Không mở file dự án trực tiếp từ thư mục đồng bộ. Chia sẻ đúng quyền, thu hồi khi xong.
- File lớn: proxy để dựng, file dự án lên cloud, review qua Frame.io/Drive, final qua WeTransfer/ổ cứng, archive khi kết thúc.
- Email chuyên nghiệp: địa chỉ nghiêm túc, tiêu đề rõ, cấu trúc đủ, file đặt tên đúng, Bcc khi gửi nhiều người.

- Mối đe dọa: mã độc (ransomware nguy hiểm nhất), phishing (lừa người chứ không hack máy), Wi-Fi giả, lộ dữ liệu. Không crack, không nhấn liên kết lạ, không đọc OTP cho ai.
- Mật khẩu: dài (16+), cụm từ, mỗi tài khoản một mật khẩu, dùng password manager (Bitwarden). 2FA bằng ứng dụng xác thực cho mọi tài khoản quan trọng; lưu mã dự phòng.
- Bảo vệ thiết bị: cập nhật, Windows Security, mã hóa ổ (BitLocker/FileVault), khóa màn hình (Win+L), Find My Device.
- Dữ liệu cá nhân: chia sẻ tối thiểu, kiểm tra cài đặt riêng tư, tách tài khoản công việc/cá nhân, tự tìm kiếm tên mình trên Google. Luật ANM 2018, NĐ 13/2023, Luật BVDLCN 2025 bảo vệ quyền của người học và quy định trách nhiệm khi người học xử lý dữ liệu người khác.

Thuật ngữ cần nhớ

Bảng 2.12 — Thuật ngữ cần nhớ

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
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
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
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

Câu hỏi ôn tập

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?
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 (làm ở nhà, nộp trước buổi sau)

Người học chọn 2 trong 7 bài, trình bày 1-2 trang Word có liên kết nguồn. Được dùng AI hỗ trợ nhưng phải kiểm chứng và ghi rõ.

1. **Cáp quang biển và Internet Việt Nam.** Việt Nam kết nối Internet quốc tế qua những tuyến cáp quang biển nào? Tại sao mỗi khi cáp đứt, mạng "chậm như rùa"? Tìm bản đồ cáp quang biển (submarinecablemap.com) và giải thích đường đi của dữ liệu khi người học xem YouTube.

2. **Phân tích một vụ lừa đảo thực tế.** Tìm một vụ lừa đảo trực tuyến được báo chí Việt Nam đưa tin trong 6 tháng gần đây (giả công an, cộng tác viên, deepfake...). Phân tích: kẻ lừa đảo đã dùng kỹ thuật tâm lý gì? Nạn nhân đã bỏ qua dấu hiệu cảnh báo nào? Nếu ở vị trí đó, người học sẽ phát hiện ở bước nào?
3. **Deepfake trong điện ảnh.** Tìm 2 ví dụ phim/chương trình đã dùng công nghệ deepfake/AI để trẻ hóa, hồi sinh diễn viên, hoặc lồng tiếng đa ngôn ngữ (ví dụ: The Irishman, Star Wars: Rogue One, Furious 7, các dự án của Flawless AI). Đánh giá: đâu là ứng dụng chính đáng, đâu là ranh giới đạo đức? Diễn viên có quyền gì với hình ảnh số của mình (tham khảo thỏa thuận SAG-AFTRA 2023)?
4. **So sánh dịch vụ đám mây cho nhóm sản xuất.** Nhóm 5 người làm phim ngắn cần 500 GB lưu trữ chung trong 6 tháng. So sánh chi phí và tính năng của 3 phương án (ví dụ: Google One 2TB chia sẻ gia đình, Dropbox Team, NAS Synology tự mua). Đề xuất phương án tối ưu và giải thích.
5. **Kiểm tra rò rỉ dữ liệu.** Truy cập haveibeenpwned.com, nhập email của người học. Ghi lại: email xuất hiện trong bao nhiêu vụ rò rỉ? Từ dịch vụ nào? Dữ liệu gì bị lộ? Tìm hiểu về 1 vụ rò rỉ lớn (ví dụ: vụ 1,3 tỷ tài khoản 2024, hoặc vụ lộ dữ liệu ở Việt Nam) và rút ra bài học.
6. **Nghị định 13/2023 và người sáng tạo nội dung.** Đọc Nghị định 13/2023/NĐ-CP (Chương II — Quyền và nghĩa vụ). Liệt kê 8 quyền của chủ thể dữ liệu. Với vai trò là người quay phim/chụp ảnh/làm nội dung, người học phải tuân thủ nghĩa vụ gì khi ghi hình người khác? Soạn một mẫu "Giấy đồng ý sử dụng hình ảnh" đơn giản.
7. **Passkey — tương lai không mật khẩu.** Passkey là gì? Hoạt động thế nào? Khác 2FA ở đâu? Những dịch vụ nào đã hỗ trợ? Hãy tạo passkey cho tài khoản Google của người học (nếu thiết bị hỗ trợ) và mô tả trải nghiệm.

Bài tập thực hành

BT1-BT3 làm trên lớp (2 tiết thực hành); BT4-BT6 làm ở nhà. Nộp ảnh chụp màn hình và file theo yêu cầu, nén thành TinHoc_Buoi02_HoTen.zip. Lưu ý: khi chụp màn hình các trang bảo mật, *che* các thông tin nhạy cảm (số điện thoại, mã dự phòng).

1. **Khám phá mạng và Internet (trên lớp, 15 phút).** (a) Mở Command Prompt, gõ ipconfig — ghi IP nội bộ, gateway, DNS. (b) Tìm IP công cộng bằng "what is my ip". (c) Gõ nslookup skda.edu.vn để xem IP của trang trường. (d) Gõ ping google.com để đo độ trễ. (e) Vào speedtest.net đo download/upload/ping. (f) Tính thời gian gửi file 5 GB với upload vừa đo. Chụp ảnh từng bước.
2. **Kiểm chứng thông tin (trên lớp, 15 phút).** Giảng viên cung cấp 3 bài đăng/tin tức (1 thật, 1 giả, 1 nửa thật nửa giả). Áp dụng SIFT cho từng tin: ghi lại từng bước điều tra, công cụ đã dùng (tìm kiếm ngược ảnh, kiểm tra

tên miền, tìm nguồn khác), và kết luận. Trình bày dưới dạng bảng 3 cột: Tin / Các bước SIFT / Kết luận.

3. **Thiết lập đám mây cho dự án (trên lớp, 15 phút).** Đưa cấu trúc thư mục dự án (BT2 chương 1) lên Google Drive hoặc OneDrive. Cài ứng dụng Desktop, chọn chế độ Stream. Chia sẻ thư mục 01_PreProduction với 1 bạn cùng lớp quyền Commenter, thư mục 05_Project_Files với quyền Editor. Bạn cùng lớp thêm 1 nhận xét và 1 file. Chụp ảnh cài đặt chia sẻ và kết quả. Sau đó thu hồi quyền chia sẻ.
4. **Rà soát bảo mật tài khoản (ở nhà).** Với tài khoản Google chính: vào myaccount.google.com > Security. (a) Chạy Security Checkup. (b) Xem "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) Xem "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.
5. **Triển khai trình quản lý mật khẩu (ở nhà).** 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.
6. **Bảo vệ thiết bị và dữ liệu cá nhân (ở nhà).** (a) Windows: kiểm tra Windows Update, Windows Security (quét toàn bộ), bật Device Encryption/BitLocker, đặt 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: đặt bài viết mặc định Bạn bè, ẩn danh sách bạn bè và số điện thoại, xem lại Apps and Websites. (d) Tự tìm kiếm tên mình trên Google (có ngoặc kép) — ghi lại 5 kết quả đầu, nhận xét danh tính số hiện tại. Chụp ảnh từng bước (che thông tin nhạy cảm), viết báo cáo 10 dòng.

Tiêu chí đánh giá bài tập

Đúng và đủ yêu cầu (40%) · Áp dụng đúng kiến thức và công cụ đã học (30%) · Trình bày rõ ràng, ảnh chụp đầy đủ, có nhận xét cá nhân (20%) · Đúng hạn, đúng định dạng (10%). Bài tập chương 2 tính vào điểm Bài tập thường xuyên (20%). Bài BT2 (kiểm chứng thông tin) và BT4 (bảo mật tài khoản) là bắt buộc.

— Hết Chương 2 —

Nguồn hình ảnh

Các ảnh trong chương lấy từ Wikimedia Commons (commons.wikimedia.org), được cấp phép tự do. Khi dùng lại cần ghi nguồn và giữ đúng giấy phép như dưới đây. Truy cập ngày 31/10/2026.

- **Hình 2.1:** Submarine cable map umap.png — Greg Mahlknecht (dữ liệu), CC BY-SA 2.0.
- **Hình 2.2:** BSNL Chennai Broadband's Wi-Fi modem.jpg — Aravind Sivaraj, CC BY-SA 3.0; Netgear-Nighthawk-AC1900-WiFi-Router.jpg — Evan-Amos, phạm vi công cộng; Netgear ProSafe 8 Port Gigabit Switch GS108 front.jpeg — Zuzu, CC BY-SA 3.0; Access Point UniFi.jpg — Sabbo91, CC BY-SA 4.0.
- **Hình 2.3:** MY DRIVE FILES.png — Hazumane, CC BY-SA 4.0 (ảnh chụp giao diện Google Drive, đã chỉnh sửa).