BECOMING A DOM · CHAPTER 3

Stay anonymous

A drawn face can't leak, but files, names, accounts, tools and payments can. Here's where the person behind a persona gets exposed, where anonymity ends, and why access to your accounts is never part of the game.

ENTRY D3 CATEGORY BECOMING A DOM CHECKED 3 NOVEMBER 2026
READING 9 MIN STEPS 6



EVIDENCE ◆ Verified ◆ Reported ◆ Vivian's field notes ◆ Unverified

This chapter is not advice for your situation.

IN 30 SECONDS

01 A drawn persona is anonymous toward the audience. She isn't anonymous toward the payout.

02 Only the persona's name belongs in anything you produce. Clean every file, then check it.

03 Small public fields, game names and wishlist names connect accounts.

04 A real dom never needs a password, a login code or a remote session.

05 If it leaks, stop, secure, keep proof and ask for help.

YOU WILL LEARN

- ✓ Who can find out who you are, and how.
- ✓ How to clean files and sites, and how to check a tool before you run it.
- ✓ Which public fields and names give a person away, for doms and for subs.
- ✓ Why anonymity ends where the money lands.
- ✓ What to do when a login request, a threat or a leak shows up.

> *I keep the persona and the person apart on purpose, and the person's side is the one I check most often.*
>
> — VIVIAN

STEP 01 OF 06

What you hide, from whom

Anonymity in 2DFD is real, but narrow. It works well toward the audience: a drawn face can't leak, a clean file carries no coordinates, and an account under a pseudonym shows no name. Compared with classic findom, the drawn character takes the face and the voice out of the deal, and the risk moves to payment platforms, social platforms and the tools used to move money. ◆

Some doms say they've been targeted by people threatening them with fake explicit pictures made to look like them. Those threats are scary even when the pictures are known to be fake. A drawn character has no real face to fake, and that's real protection. ◆

Secrecy has a cost. In a study of findommes, participants named secrecy among the most negative parts of the work. ◆ Keep at least one person you trust who knows what you do.

Who could find out who you are

◆	How you can leak	What helps
Subs	A bio line, a game name, a name on a wishlist	Public fields that match each other and hold no real-life detail
Platforms	Phone checks, linked accounts, file metadata	Clean exports, one purpose per account
Payment company	ID papers and a bank account	Accept it, and plan for it from the start
Family or employer	A chat left open, a shared computer	A separate profile, a locked screen
Other doms	A name seen on two pages, a handle found in a file	A handle you're fine being recognised by

This map is from my own experience. There's no study behind it. ◆

Files, sites and tools

Only the persona's name goes in anything you produce: files, file names, commits, metadata and screenshots. Never a personal name, an e-mail address or a system path that contains a user name. ◆

Images carry traces: location data, colour profiles, comments, provenance records, prompts stored in text chunks and extra bytes. Videos carry a date, the name of the program and the name of the encoder. Clean every export, then reread the file, and if anything's left, don't post it. Clean even when you start clean, because an encoder can add a profile on its own. Test your checker with odd cases, because a hidden note in an unexpected spot once slipped through mine. Treat every picture as copyable too, since anyone can take a screenshot. ◆

Publish an image

0 OF 5 DONE

- [ ] 01 Export the file from your tool.
- [ ] 02 Strip it: location, profiles, comments, prompts and extra bytes.
- [ ] 03 Reread the stripped file and compare it with a clean sample.
- [ ] 04 If anything's left, stop and fix the cause, not the file.
- [ ] 05 Only then post it.

Tick the lines as you go. Your ticks stay on this page only and clear when you leave it.

A site can leak through how it’s built. Serve everything from the site’s own host, with no third-party fonts, trackers or scripts, so only the host sees a visit. Check it from the outside: old versions of a site can stay reachable at hosting addresses you’ve forgotten. Browser safety filters can flag new adult-themed domains early, so test the name and keep a backup. ◆

Code leaks too. Make commits under the persona’s name and in UTC, because a local time offset shows where the author lives. Open a code-hosting account with a pseudonym for both the name and the e-mail, because every change stays in the history. Before you give a tool to others, take out any name, signature and default picture, and strip the source, comments and leftover handles, or someone can repackage it with something added. ◆

Secrets never go through a chat. Type a token or key into a masked prompt in your own terminal, never into a commit, screenshot or message, and send access keys privately so they can be revoked. ◆

A tool can be harmless in code and still unsafe in practice. Check what it sends and to whom, check its defaults as well as its screen, and test it in a virtual machine with no personal network. Don’t run an unknown program on your main computer. Avoid any tool that builds an ID from the computer name or the account name. A safer design starts with everything off, a whitelist, a random ID, a short history and a control channel by invitation only. ◆

Anonymous confession features are only anonymous toward other members. The platform and the host still have the data. ◆

Accounts, names and public fields

Public fields leak more than files. One careless bio line on a related account can show that the person behind a persona isn't who the persona says. A game or stream name that looks like the persona's name, or points back to an old dispute, can do the same. ◆ Read every public field of every linked account the way a stranger would.

People who run personas often have several accounts. Platform terms may forbid multiple accounts, or a new account after a ban, and a second account puts the first one at risk. ◆ Don't borrow someone else's phone number for a check. It drags a person who has nothing to do with this into adult activity. ◆

Don't confirm or explain links between personas. When someone asks about a persona's contacts or second identities, deflect. Never publicly link a handle you found in a tool's files to a persona unless the person said so in their own words, because that's doxxing. Exposing a bad actor also invites revenge, like mass reports from accounts the rival controls. If you show a mentor or a peer anything, show the persona account, never the personal one. ◆

Purging messages and blocking contacts keeps the persona apart from the person, but it also wipes out what you could learn from. ◆ Deleting chats after every send is different, because it can be a sign of the spiral. See The spiral.

If you're a sub

Sender names can show on a public wishlist, and doms look at each other's pages. Use a handle you're fine with several doms seeing. Keep a separate account for adult servers, and check who else is in a server before you join, because a server you have in common with someone can expose you. On

a shared computer, lock the screen or close the chat, and use a separate profile. ◆

Your name, your address, your workplace and your family are a fair boundary. A dom who needs them isn't playing a game. Physical gifts break anonymity both ways, so the safe default is no addresses at all, or a neutral forwarding or retail service. ◆

STEP 04 OF 06

Money is the weak point

Anonymity ends at the payout. In my experience a card processor or an adult payment company ties the persona to a legal identity: ID documents, a business registration and a bank account in the company's country. An account opened in a real name carries any ban with it, and the ban follows the real person. ◆

The persona is a mask toward the audience and the platforms, never toward the company that pays you. Partial or false details at a processor won't make you anonymous. They get accounts closed and money held, and a sub's payment can disappear with them. ◆ The authors of a study of findommes flag fraud, including identity fraud, as a remaining risk in this field. ◆

A persona's tools hold no names, e-mail addresses or cards. A card stays with the processor. Test any payment flow with a fake provider first, then in the provider's test mode with its published test cards, and type a real key only in your own terminal. ◆ For the full picture, see Getting paid.

MYTH	FACT
~~A drawn persona makes everything around her anonymous.~~	It protects the face and the voice. The payout, the small public fields and the tools you run still point to a person. ◆
MYTH	FACT
~~Throwaway cards and partial details get around a processor's checks.~~	They get accounts closed and money held, and the account follows the real identity. ◆

STEP 05 OF 06

Access is never part of the game

A real dom never needs your password. Passwords and one-time codes are keys to your identity, and a promise doesn't protect you. ◆ A US cybersecurity alert advises people not to hand control of a computer or phone to a stranger. ◆ A remote-access vendor states that it does not offer remote support services, so a caller claiming to be its support isn't genuine. ◆

In this scene the same request shows up inside the game. Press reports describe some doms blackmailing subs. ◆ A first-person account says threats of exposure are a common punishment from financial doms. ◆ A login handed over as a gesture of trust is really about control, and a fake dom would ask for exactly the same thing. ◆

VIVIAN'S FIELD NOTES

I track how these requests are worded. The language of trust and the language of a scam overlap completely. When someone says a password proves you're serious, the request itself is the red flag, whatever they mean by it. A dom who means well doesn't need your password, and one who doesn't will say the same words.

◆

RED FLAGS

Access requests

- A dom asks for your password as proof you're honest.
- A dom asks for the one-time code just sent to your phone or e-mail.
- A dom asks for a remote desktop session "to supervise", and adds that you can always quit.
- A dom logs you out of your own accounts, or keeps them open "for you".
- A dom asks for access as the price of forgiveness.

Counter. Say no once, calmly. Offer a screenshot or an export instead. If you already shared anything, change the password and sign out of every session. Don't argue.

Pressure around privacy

WHAT THEY SAY OR DO

01 *"Prove you are honest: give me your login."*

THE COUNTER

A login proves nothing and opens everything. Refuse and show a screenshot instead. ◆

WHAT THEY SAY OR DO

02 *"Why would you want to do this alone?"*

THE COUNTER

Asking you to justify your privacy makes you defend a normal boundary. Say it once: "because I want to" is enough. ◆

WHAT THEY SAY OR DO

03 *"I only want access because I care."*

THE COUNTER

Wanting into someone's account because it feels special is a control pattern. Say no. ◆

WHAT THEY SAY OR DO

04 *"That dom is not who she says she is. Leave her."*

THE COUNTER

Exposing someone to win you over isolates you. Ask why her identity is the argument. ◆

It works the other way too. Giving anyone, even a mentor you trust, full access to the account where your subs talk is risky. The subs can't speak freely, and the helper can step into conversations. If you share access, tell the subs, exclude specific conversations, and remove the helper's sessions when trust drops. ◆

TRY IT

A dom asks for a code

You sent a tribute and told a dom you also pay others. She says you can prove you're honest by reading out the code that just came by text, and promises she won't do anything harmful. What do you do?

A Refuse, offer a screenshot, and change your passwords if you shared anything before

The right answer. Right. A code opens your account to whoever has it. A promise doesn't protect you.

B Read the code, since she promised not to do anything harmful

Not this one. You can't check the promise, and you can't take the code back.

C Give her your password instead of the code

Not this one. A password is the bigger key. The same rule applies.

When it leaks

Rumours and screenshots travel fast. A rumour that a dom is secretly a sub can cost her subs, and private images can spread through a shared server before any apology comes. ◆ Keep private images and chats out of any shared space.

If your identity leaks

0 OF 5 DONE

- [ ] 01 Stop. Don’t confirm or deny any real-life detail.
- [ ] 02 Secure your accounts: change passwords and sign out of every session.
- [ ] 03 Save proof with dates before you block anyone.
- [ ] 04 Report the account to the platform. Don’t pay a blackmailer, and don’t send more material.
- [ ] 05 Tell one person you trust, and read Where to get help.

Never hand over

Password

Never. A real dom never needs it.

One-time code

Never. It opens your account.

Address

Not without a neutral forwarding service.

Card number

Never. The card stays with the processor.

TRY IT

Check yourself

QUESTION 1 OF 2

Where does anonymity end for a dom?

- ◯ At the bio
- ◯ At the payout
- ◯ At the first post

Answer. At the payout. A processor ties the persona to a legal identity.

QUESTION 2 OF 2

A dom says you need a reason for your privacy. What is that?

- ◯ A fair question
- ◯ A pressure pattern
- ◯ A required form

Answer. A pressure pattern. A boundary needs no proof.

REMEMBER IT

- Only the persona's name goes in anything you produce.
- Clean every file, then check it.
- Public fields and game names connect accounts.
- Anonymity ends at the payout.
- A real dom never needs your password or a code.
- If it leaks, stop, secure, keep proof and ask for help.

SOURCES AND EVIDENCE

Check it

Every claim with its evidence level and its sources.

EVIDENCE LEVELS

Verified	Checked against the original source.
Reported	Stated by a serious secondary source read in full.
Community	Widely said in the scene; no document proves it.
Vivian's field notes	First-hand experience, not a study.
Unverified	Plausible, not proven yet.

01 It works well toward the audience: a drawn face can't leak, a clean file carries no coordinates, and an account under a pseudonym shows no name.

◆

02 Compared with classic findom, the drawn character takes the face and the voice out of the deal, and the risk moves to payment platforms, social platforms and the tools used to move money.

◆

03 Those threats are scary even when the pictures are known to be fake.

◆

04 A drawn character has no real face to fake, and that's real protection.

◆

05 In a study of findommes, participants named secrecy among the most negative parts of the work.

◆

Findommes, Cybermediated Sex Work, and Rinsing (McCracken and Brooks-Gordon, Sexuality Research and Social Policy 18(4), 837-854, DOI 10.1007/s13178-021-00609-3) (https://www.ebi.ac.uk/europepmc/webservices/rest/PMC8418458/fullTextXML)

Archive (https://web.archive.org/web/20261016030740/https://pmc.ncbi.nlm.nih.gov/articles/PMC8418458/)

Accessed 3 November 2026

06 There's no study behind it.

◆

07 Never a personal name, an e-mail address or a system path that contains a user name.

◆

08 Videos carry a date, the name of the program and the name of the encoder.

◆

09 Clean every export, then reread the file, and if anything's left, don't post it.

◆

10 Clean even when you start clean, because an encoder can add a profile on its own.

◆

11 Test your checker with odd cases, because a hidden note in an unexpected spot once slipped through mine.

◆

12 Treat every picture as copyable too, since anyone can take a screenshot.

◆

13 Serve everything from the site's own host, with no third-party fonts, trackers or scripts, so only the host sees a visit.

◆

14 Check it from the outside: old versions of a site can stay reachable at hosting addresses you've forgotten.

◆

15 Browser safety filters can flag new adult-themed domains early, so test the name and keep a backup.

◆

16 Make commits under the persona's name and in UTC, because a local time offset shows where the author lives.

◆

17 Open a code-hosting account with a pseudonym for both the name and the e-mail, because every change stays in the history.

◆

18 Before you give a tool to others, take out any name, signature and default picture, and strip the source, comments and leftover handles, or someone can repackage it with something added.

◆

19 Type a token or key into a masked prompt in your own terminal, never into a commit, screenshot or message, and send access keys privately so they can be revoked.

◆

20 Check what it sends and to whom, check its defaults as well as its screen, and test it in a virtual machine with no personal network.

◆

21 Don’t run an unknown program on your main computer.

◆

22 Avoid any tool that builds an ID from the computer name or the account name.

◆

23 A safer design starts with everything off, a whitelist, a random ID, a short history and a control channel by invitation only.

◆

24 The platform and the host still have the data.

◆

25 One careless bio line on a related account can show that the person behind a persona isn’t who the persona says.

◆

26 A game or stream name that looks like the persona’s name, or points back to an old dispute, can do the same.

◆

27 Platform terms may forbid multiple accounts, or a new account after a ban, and a second account puts the first one at risk.

◆

28 It drags a person who has nothing to do with this into adult activity.

◆

29 When someone asks about a persona's contacts or second identities, deflect.

◆

30 Never publicly link a handle you found in a tool's files to a persona unless the person said so in their own words, because that's doxxing.

◆

31 Exposing a bad actor also invites revenge, like mass reports from accounts the rival controls.

◆

32 If you show a mentor or a peer anything, show the persona account, never the personal one.

◆

33 Purging messages and blocking contacts keeps the persona apart from the person, but it also wipes out what you could learn from.

◆

34 Use a handle you're fine with several doms seeing.

◆

35 Keep a separate account for adult servers, and check who else is in a server before you join, because a server you have in common with someone can expose you.

◆

36 On a shared computer, lock the screen or close the chat, and use a separate profile.

◆

37 A dom who needs them isn't playing a game.

◆

38 Physical gifts break anonymity both ways, so the safe default is no addresses at all, or a neutral forwarding or retail service.

◆

39 In my experience a card processor or an adult payment company ties the persona to a legal identity: ID documents, a business registration and a bank account in the company's country.

◆

40 An account opened in a real name carries any ban with it, and the ban follows the real person.

◆

41 The persona is a mask toward the audience and the platforms, never toward the company that pays you.

◆

42 They get accounts closed and money held, and a sub's payment can disappear with them.

◆

43 The authors of a study of findommes flag fraud, including identity fraud, as a remaining risk in this field.

◆

Findommes, Cybermediated Sex Work, and Rinsing (McCracken and Brooks-Gordon, Sexuality Research and Social Policy 18(4), 837-854, DOI 10.1007/s13178-021-00609-3) (https://www.ebi.ac.uk/europepmc/webservices/rest/PMC8418458/fullTextXML)

Archive (https://web.archive.org/web/20261016030740/https://pmc.ncbi.nlm.nih.gov/articles/PMC8418458/)

Accessed 3 November 2026

44 A card stays with the processor.

◆

45 Test any payment flow with a fake provider first, then in the provider's test mode with its published test cards, and type a real key only in your own terminal.

◆

46 The payout, the small public fields and the tools you run still point to a person.

◆

47 They get accounts closed and money held, and the account follows the real identity.

◆

48 Passwords and one-time codes are keys to your identity, and a promise doesn't protect you.

◆

49 A US cybersecurity alert advises people not to hand control of a computer or phone to a stranger.

◆

IC3 Issues Alert on Tech Support Fraud (https://www.cisa.gov/news-events/alerts/2018/03/29/ic3-issues-alert-tech-support-fraud)

Archive (https://web.archive.org/web/20250716102123/https://www.cisa.gov/news-events/alerts/2018/03/29/ic3-issues-alert-tech-support-fraud)

Accessed 3 November 2026

50 A remote-access vendor states that it does not offer remote support services, so a caller claiming to be its support isn't genuine.

◆

TeamViewer and scamming (https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/teamviewer-and-scamming/)

Archive (https://web.archive.org/web/20260519191922/https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/teamviewer-and-scamming/)

Accessed 3 November 2026

51 Press reports describe some doms blackmailing subs.

◆

[a former participant] has seen men left broke and hungry from 'paying women to talk to them' (https://www.sbs.com.au/news/the-feed/article/the-online-kink-thats-leaving-some-men-homeless-bankrupt-and-normalising-suffering/vocm5xt30)

Archive (https://web.archive.org/web/20251123124217/https://www.sbs.com.au/news/the-feed/article/the-online-kink-thats-leaving-some-men-homeless-bankrupt-and-normalising-suffering/vocm5xt30)

Accessed 3 November 2026

52 A first-person account says threats of exposure are a common punishment from financial doms.

◆

Diary of a Financial Dominatrix, part one (https://www.theskinny.co.uk/sexuality/deviance/diary-of-a-financial-dominatrix-part-one)

Archive (https://web.archive.org/web/20200805021033/https://www.theskinny.co.uk/sexuality/deviance/diary-of-a-financial-dominatrix-part-one)

Accessed 3 November 2026

53 A login handed over as a gesture of trust is really about control, and a fake dom would ask for exactly the same thing.

◆

54 I track how these requests are worded. The language of trust and the language of a scam overlap completely. When someone says a password proves you're serious, the request itself is the red flag, whatever they mean by it. A dom who means well doesn't need your password, and one who doesn't will say the same words.

◆

55 Refuse and show a screenshot instead.

◆

56 Say it once: "because I want to" is enough.

◆

57 Say no.

◆

58 Ask why her identity is the argument.

◆

59 If you share access, tell the subs, exclude specific conversations, and remove the helper's sessions when trust drops.

◆

60 A rumour that a dom is secretly a sub can cost her subs, and private images can spread through a shared server before any apology comes.

◆