SCAMS · CHAPTER 5

Fake tools

A fake tool is an extension or app that does more than its page says, or makes it hard to stop. In my experience few are malware. Most are working code with a hidden price.

FILE X5 CATEGORY SCAMS CHECKED 3 NOVEMBER 2026 READING 7 MIN
SECTIONS 5 STATUS OPEN

EVIDENCE ◆ Verified ◆ Reported ◆ Vivian's field notes

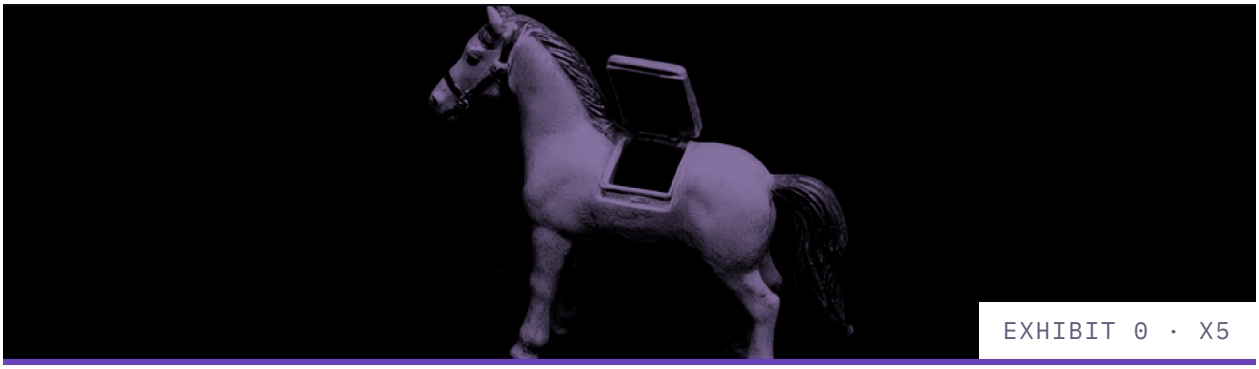


EXHIBIT 0 · X5

IN 30 SECONDS

01 A tool can send, reach or change more than its page says, and it stays on your computer until you remove it.

02 Most of the harm comes from design: a tool without a limit, a running total or a stop that always works.

03 A tool that's harmless today and could turn harmful after one update needs a different verdict from "malware".

04 Remote control, buying in the background and tools that act as you are the biggest risks.

05 A feature built to make the next payment harder to refuse is a reason to leave.

YOU WILL LEARN

- ✓ What a tool can do that its page doesn't say.
- ✓ How to word a verdict so it says what was read.
- ✓ The pressure features to recognise, and the minimum a safe tool shows.
- ✓ Why remote access and borrowed sign-ins are a red line.
- ✓ Why protection inside an app is weak, and what that means for you.

> *Some tools break their promises. Others keep them and still cost you more than you meant to spend. This chapter shows you what to look for, so you can say no before you install. To check a specific tool, use Check a tool before you install it.*
>
> — VIVIAN

PART 01

What a tool can do that its page doesn't say

In this wiki a fake tool is any extension or app that sends more than it says, acts beyond what you agreed to, or makes it hard to stop. In my experience few of them are malware, and most are working code with a hidden price or no way out.

A tool can go further than its page in four ways.

- *It sends more.* A tool can build a machine identifier from your computer's name and your account name, send it to its server and show it on screen. That exposes who you are.
- *It reaches further.* A tool that keeps your signed-in session and buys in the background takes away the pause between decisions. The only brake left is a limit you set beforehand.
- *It changes later.* An updater can fetch new files after you've stopped paying attention.
- *It skips consent.* A roleplay app can look impressive and still lack a safe word, a consent screen and aftercare, and some of its promised content may never arrive. A dom who uses consent tools shows them: a stop control, a log of what she can see, and a clear line between teasing and harming.

> VIVIAN'S FIELD NOTES
>
> *A tool that stays installed stays a risk. If you ignore it today and its maker pushes a harmful update tomorrow, you're exposed, and a maker could wait until lots of people have installed it. Removing the tool is the simplest way out, and once it's gone it can't drain you.*

PART 02

Not malicious today

Calling a tool malware before reading all of it can lead to a false alarm you have to take back. ◆ The sequence below is an invented example, because a correction teaches more than an alarm.

A verdict that matches what was read (invented example)

1 **First reading**

A quick look at a control app suggests the worst: stored sign-in tokens and a link to a remote server. ◆

2 **Full reading**

Reading the whole source, the updater and every network call included, shows what's really sent and to whom. ◆

3 **The finding**

If the updater can push any file and the tokens sit on the same computer, one update could take everything. ◆

4 **The wording**

The honest verdict names what was read and what could change: harmless today, risky after one update. ◆

A finding like that is narrower than “malware” and still serious. A design risk is the usual kind of danger, and it needs a verdict worded to match. ◆ Check a tool before you install it gives the words to use, from mildest to strongest.

CLAIM 1

MYTH

“If a tool isn’t malware, it’s fine.”

FACT

A tool can be free of malware and still send identifying details about your computer to its server. Its code can be harmless and it can still be unsafe to use. ◆

CLAIM 2

MYTH

“A tool has a stop if you can close the program.”

FACT

Some tools can only be stopped by force-closing the app or turning the computer off. A stop that depends on your willpower is no stop. Force-closing always works, so know how to do it, but a visible stop that works in every state has to exist too. ◆

PART 03

Designs that push you to spend

A limit set in advance is your first brake. The features below work against it, and each one makes the next payment harder to refuse. Press reports guilt-based pressure from some dominants, and a former participant describes men

who sold cars, took on debt and worked second jobs. ◆ A tool that automates the same guilt is using the same tactic.

RED FLAGS

Designs to refuse

- A forced respin, or a prompt you can't close without choosing.
- Minimum amounts that go up after each round.
- A sentence you have to type to continue.
- A mascot that sulks, scolds or pleads until you act.
- A hidden total, or a charged amount that's different from the one shown.
- A lock that only opens on payment, or a tool that can't be removed.
- Overnight modes, or targeting your payday and your balance.

Counter. Close it and leave. These features are there to earn from your next send. Assume a tool has none of the protections below until you see them.

The minimum a safe tool shows

◆	What a safe tool does	If it's missing
Start	Arrives switched off, with one master switch	Don't install
Scope	Does one named thing on one named site	Ask for it to be narrowed, or leave
Total	Shows a running total and counts only confirmed payments	Don't install
Limit	Enforces the limit you set in advance	Set a spending limit at your bank
Wait	Spaces payments with a cooldown	Ask for it
Stop	One visible stop that works in every state	Don't install
Removal	Can be removed in one click	Don't install

Safe design often means earning less, and a tool that has all of this has given something up. Even then, a determined person can get around a blocking or

draining extension, so a tool should never be your only control. ◆ See Breaks that hold.

PART 04

Remote control and tools that act as you

A remote-session hands your computer to someone else, and a US government alert advises people not to give control of their computers or mobile devices to any stranger. ◆ The full rule, with the lines people use to talk you into it, is in Check a tool before you install it.

A hub-style app can add remote actions: making accounts follow, post or send, sending files, or reaching a terminal. If it does, one flaw lets the author, or anyone, act through every installed copy. An app like that needs an independent security check before release, and anyone who finds a flaw like that should tell the maker and not use it. ◆

RED FLAGS

Tools that act as you

- It likes, follows or posts from your accounts.
- It keeps your signed-in session and buys in the background.
- It's advertised as getting around your bank's confirmation step.
- It asks you to hand over a password, a login code or a connection code.

Counter. Refuse. Automation on your account can get it banned and can flag the dom's account for botting, and you're the one who takes the consequences. A version built to get around your own bank's check removes a brake that protects your money.

Sign-ins and second steps

What is a session token?

ANSWER

A stored credential that keeps a program signed in to your account without asking for your password. ◆

What can its holder do?

ANSWER

Act as you, without the password and without the second step. ◆

Does a second step protect a session that's been taken?

ANSWER

No. The second step is asked at sign-in, and a taken session has already signed in. ◆

After a doubtful tool, what do you do?

ANSWER

Sign out everywhere, then change your passwords from a different computer. ◆

Protection that doesn’t protect

> VIVIAN’S FIELD NOTES
>
> *Makers encrypt images and scramble code to keep copies away. The key and the logic still ship inside the app, so a person with patience, ordinary tools or an assistant can read all of it. Whatever your computer can open, someone can extract. Scrambling stops casual copying and does nothing against a determined reader. That openness works for you too: a tool you can inspect is a tool you can check, so I prefer those.*
>
> ◆

A build step can change what a tool does, so the build that ships may not be the one that was tested. A wrong version can charge a different amount from the one it shows. A test switch that skips the payment step, a bypass, must never leave the maker’s computer. ◆ Makers: the list is in Check a tool before you install it.

A tool can also trap the people it’s meant to serve. A bug, an overlay or a lock can leave a sub with no way to remove a tool. A lock that only opens on payment is a paid exit and a reason to leave, because it turns a game you agreed to into a harm you didn’t. ◆ A maker needs an automatic unlock, and no overlay that covers the stop.

If you’ve installed a tool you now doubt, the steps are in Check a tool before you install it. If money has left, go to If you already sent.

TRY IT

Which of these tools passes?

Five tools are offered to you. On this list alone, only one is acceptable. Which one?

A A control app that can only be stopped by turning the computer off

Not this one. A stop that depends on your willpower is no stop.

B A background buyer that keeps your session and shows no running total

Not this one. The only brake left is a limit you can't watch working.

C An app whose mascot sulks until you spin again

Not this one. A guilt line built into a tool is pressure by design.

D An app that needs a remote session to finish setting up

Not this one. Full control of your computer can't be taken back.

E A tool that arrives off, does one named thing on one named site, shows a running total and has a stop that works in every state

The right answer. It passes this list. It still needs the full check, and your own limit.

REMEMBER IT

- In my experience few fake tools are malware. Most are working code with a hidden price or no way out.
- A verdict says what was read: “not malicious today” doesn’t mean “safe”.
- A feature built to make the next send harder to refuse is a reason to leave.
- A safe tool arrives off, shows a total, enforces your limit and stops in every state.
- Nobody who plays fair needs remote control of your computer or your sign-in.
- Whatever your computer can open, someone can read. Prefer tools you can inspect.

SOURCES AND EVIDENCE

Check it

Every claim with its evidence level and its sources.

01 In my experience few of them are malware, and most are working code with a hidden price or no way out.

02 A tool can go further than its page in four ways.

03 That exposes who you are.

◆

04 The only brake left is a limit you set beforehand.

◆

05 An updater can fetch new files after you've stopped paying attention.

◆

06 A dom who uses consent tools shows them: a stop control, a log of what she can see, and a clear line between teasing and harming.

◆

07 A tool that stays installed stays a risk. If you ignore it today and its maker pushes a harmful update tomorrow, you're exposed, and a maker could wait until lots of people have installed it. Removing the tool is the simplest way out, and once it's gone it can't drain you.

◆

08 Calling a tool malware before reading all of it can lead to a false alarm you have to take back.

◆

09 A quick look at a control app suggests the worst: stored sign-in tokens and a link to a remote server.

◆

10 Reading the whole source, the updater and every network call included, shows what's really sent and to whom.

◆

11 If the updater can push any file and the tokens sit on the same computer, one update could take everything.

◆

12 The honest verdict names what was read and what could change: harmless today, risky after one update.

◆

13 A design risk is the usual kind of danger, and it needs a verdict worded to match.

◆

14 Its code can be harmless and it can still be unsafe to use.

◆

15 Force-closing always works, so know how to do it, but a visible stop that works in every state has to exist too.

◆

16 Press reports guilt-based pressure from some dominants, and a former participant describes men who sold cars, took on debt and worked second jobs.

◆

[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

17 Safe design often means earning less, and a tool that has all of this has given something up.

◆

18 Even then, a determined person can get around a blocking or draining extension, so a tool should never be your only control.

◆

19 A remote-session hands your computer to someone else, and a US government alert advises people not to give control of their computers or mobile devices to any 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

20 If it does, one flaw lets the author, or anyone, act through every installed copy.

◆

21 An app like that needs an independent security check before release, and anyone who finds a flaw like that should tell the maker and not use it.

◆

22 A stored credential that keeps a program signed in to your account without asking for your password.

◆

23 Act as you, without the password and without the second step.

◆

24 The second step is asked at sign-in, and a taken session has already signed in.

◆

25 Sign out everywhere, then change your passwords from a different computer.

◆

26 Makers encrypt images and scramble code to keep copies away. The key and the logic still ship inside the app, so a person with patience, ordinary tools or an assistant can read all of it. Whatever your computer can open, someone can extract. Scrambling stops casual copying and does nothing against a determined reader. That openness works for you too: a tool you can inspect is a tool you can check, so I prefer those.

◆

27 A build step can change what a tool does, so the build that ships may not be the one that was tested.

◆

28 A wrong version can charge a different amount from the one it shows.

◆

29 A test switch that skips the payment step, a bypass, must never leave the maker's computer.

◆

30 A bug, an overlay or a lock can leave a sub with no way to remove a tool.

◆

31 A lock that only opens on payment is a paid exit and a reason to leave, because it turns a game you agreed to into a harm you didn't.

◆



Free, confidential helplines exist in most countries.

Find a helpline →

Nothing here is financial, legal or medical advice for your situation.