



FALLEN EXPOSURE
THE LIGHT WAS ALWAYS THERE

EVIDENCE LOCKER
FILE 002
PROTECTION BRIEF
OCT 2026

CASE OPEN

BE WISE AS SERPENTS · HARMLESS AS DOVES

BLACK OCTOBER

Guarding your home online: a sourced look at “The Internet Is Being Hacked” and a family protection plan

A fact-checked brief on Peter Yang's video (YouTube, Oct 22, 2026)

What actually happened · each claim checked · what the video leaves out

Family protection checklist · trusted resources

“Nevertheless we made our prayer to our God, and because of them we set a watch against them day and night.”

NEHEMIAH 4:9 · NKJV

SECTION 1

01 AT A GLANCE

Six things to know before you panic, share the video, or hand your passwords to anyone.

- 1 **The week was real.** Between about Oct 16 and 22, 2026, a cluster of serious security disclosures landed at once, including critical PHP flaws (“php2shell”), a maximum-severity GitLab bug, and breaches at the developer platforms Railway and Zeabur, Quest Diagnostics, and a California student-testing contractor. Newsrooms picked up the nickname “Black October.” **VERIFIED**
- 2 **The government warning was real, but narrower than it sounded.** CISA told *organizations* running PHP to patch immediately, and said those that cannot patch should take PHP systems offline until they can. That is advice to website operators, not an order to every household. **PARTLY VERIFIED**
- 3 **“Rogue AI agents in bank accounts” needs context.** Axios did report that banks are finding AI agents they never authorized inside customer accounts. In most reported cases, though, customers had handed the agent their own login. It is not evidence of a wave of criminal account takeovers. **NEEDS CONTEXT**
- 4 **Most of the video’s six steps are sound.** Disconnect unused apps, use a password manager, turn on stronger two-factor sign-in, update your software, and distrust “you’ve been breached” messages. These match CISA’s current advice for households. **VERIFIED**
- 5 **Two cautions.** The video leaves out *passkeys*, which CISA rates above authenticator apps. It also encourages letting an AI agent click through your email and accounts, which carries real risk: hidden instructions in a web page or email can redirect an agent.
- 6 **The discernment takeaway.** Scripture calls for watchfulness without fear: “A prudent man foresees evil and hides himself” (Prov 22:3), and “God has not given us a spirit of fear” (2 Tim 1:7). Take a few concrete steps, pray, and get back to ordinary life, as Nehemiah did.

How to read this brief

VERIFIED means we confirmed the claim in an official or primary source. **PARTLY VERIFIED** means the core is true but the video overstates or simplifies it. **NEEDS CONTEXT** means the claim is accurate on its face but misleading without more information. **UNVERIFIED** means we could not confirm it. Research was gathered on Oct 23, 2026 with a live-search research tool. Every official notice and news report behind a “Verified” claim was then opened and read by hand, except Reuters, which blocked access (see Sources). This brief is not technical or legal advice; for a business or church system, consult your web host or IT provider. Scripture is quoted from the NKJV.

02 THE VIDEO UNDER REVIEW

A 15-minute “emergency” tutorial from a tech and AI creator, posted the day after the PHP alert.

FIELD	DETAIL
Title	“The Internet Is Being Hacked. 6 Things You Need To Do Now”
Creator	Peter Yang (YouTube @PeterYangYT; X @petergyang), who publishes practical AI tutorials and a newsletter
Published	Oct 22, 2026 · 14 min 46 s
URL	youtube.com/watch?v=nXMISq4aFBg
Our copy	We reviewed the video’s full spoken transcript (from its public YouTube page) and its description, which includes a free “security reviewer” AI prompt.

WHAT THE VIDEO SAYS

Yang opens by saying “the internet is being hacked right now,” with “at least 12 security fires” that week, half of them the day before. He highlights two: the U.S. government telling every organization running PHP to “update right away or take their system offline,” and an Axios report that major banks are “finding AI agents nobody authorized inside customer accounts.” He explains the moment as an arms race: code written by humans before AI contains old vulnerabilities, and AI now lets both attackers and defenders find them quickly.

He shares a personal story: he received an alert that “an agent on a Linux machine was reading my emails,” could not tell which of his AI agents caused it, and spent two hours locking down his accounts. He then gives six steps and offers a prompt that has an AI assistant audit your accounts and produce a personal security report.

THE SIX STEPS, IN HIS WORDS

1 · DISCONNECT UNUSED APPS Review apps linked to your Google account (he had 47) and remove the ones you don’t use. He suggests an AI agent can do the clicking for you.	3 · TWO-FACTOR VIA AN APP Text-message codes are “not secure” and can be intercepted. Use an authenticator app such as Google Authenticator.	5 · UPDATE SOFTWARE Ask an AI to scan your computer and projects for outdated or vulnerable packages, then approve the updates.
2 · USE A PASSWORD MANAGER Unique passwords everywhere. He uses 1Password (about \$50 a year, 14-day trial) and its Watchtower audit, says he is not sponsored, and mentions the new “1Password for Agents.”	4 · ROTATE OR RETIRE API KEYS For people who build apps: rotate all active keys and retire the unused ones.	6 · DISTRUST BREACH EMAILS & CALLS Expect a wave of phishing that uses the news. Check the sender’s address and hover over links before clicking.

Fair summary of the video

The video is a practical, good-faith tutorial. It is not a conspiracy video, and most of its advice is mainstream. Its weaknesses are a hotter headline than the facts support (“the internet is being hacked”), some compressed news claims, and heavy reliance on AI agents to do security work. Those are judgments about the content, not about the creator’s motives.

SECTION 3

03 THE CLAIMS, CHECKED

Each news claim in the video, tested against official statements and named reporting.

CLAIM IN THE VIDEO	STATUS	WHAT THE RECORD SHOWS
“At least 12 security fires this week. Half of them happened just yesterday.”	PARTLY VERIFIED	A genuine cluster of incidents landed Oct 16–22, with the densest disclosures on Oct 21. There is no official count of “12”; the number matches a viral list posted on X on Oct 22. Several items were older problems disclosed that week rather than new attacks. Confirmed items are listed below.
The government told every organization running PHP to update right away or take systems offline.	PARTLY VERIFIED	CISA’s Oct 21 alert, “Critical Vulnerabilities in PHP Require Immediate Patching,” covers CVE-2026-109618 and CVE-2026-109619 and urges updating to PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35. It says: “Organizations that cannot update immediately, or that continue to use PHP 8.1 or earlier unsupported versions, should take PHP-based systems offline until they can be patched or updated.” The offline step is <i>conditional advice</i>, not a blanket order. The NSA’s advisory the same day said the same: “If an immediate update is not feasible, it is recommended that organizations take the system offline until it can be fully mitigated.”
Axios reported that major banks are finding AI agents nobody authorized inside customer accounts, some acting independently.	NEEDS CONTEXT	Axios (Madison Mills, Oct 22): “Scoop: Unvetted AI agents are accessing U.S. bank accounts.” The same report says these are generally agents using the customer’s own permission and login, which breaks bank rules. In some other cases banks saw agents act without the user’s instruction, such as calling a bank’s call center. The Axios reporter told CBS News these agents “weren’t going rogue or hacking customer accounts and depleting their funds” (CBS’s paraphrase). “Unauthorized” mostly means <i>not approved by the bank</i>.
Old, human-written code is full of bugs; AI now finds them; it is an arms race.	VERIFIED	Wiz Research, which helped disclose php2shell, says the flaws sat in PHP for over a decade and that frontier AI models “substantially reduced” the barrier to exploiting them. The Guardian (Oct 23) quotes Anthropic’s deputy CISO Jason Clinton warning of a “vulnerability tsunami,” and The Atlantic (Oct 23) quotes Palo Alto Networks’ Sam Rubin saying the internet is entering a “valley of pain.” The video’s unnamed “security expert” could not be matched to one specific quote.
He got an alert that an agent on a Linux machine was reading his email.	UNVERIFIED (personal)	He posted about it on X the same day with a screenshot. Only he can confirm what happened in his accounts. His point that cloud AI agents run on Linux machines, so an alert may not identify which agent acted, is reasonable.
People are calling it “Black October.”	VERIFIED (as a nickname)	The Guardian (“what’s being called ‘Black October’”) and The Atlantic (“which some security experts are calling ‘Black October’”) both used it on Oct 23, and other outlets picked it up. Reporting traces it to social media posts around Oct 22. It is not an official government name.

CLAIM IN THE VIDEO	STATUS	WHAT THE RECORD SHOWS
Text-message (SMS) codes are not secure; use an authenticator app.	PARTLY VERIFIED	CISA says SMS and voice codes are vulnerable to phishing, interception and SIM swaps, and that this form “should only be used as a last resort.” An authenticator app is better. But CISA ranks phishing-resistant FIDO/WebAuthn sign-in (hardware security keys and passkeys) above authenticator apps, because a fake login page can still trick you into typing an app code. The video does not mention passkeys.
1Password costs about \$50 a year, has a 14-day trial and Watchtower, and “1Password for Agent Platform” lets an agent sign in without seeing your password.	PARTLY VERIFIED	Pricing checks out (\$3.99/month billed yearly, about \$48; 14-day free trial; Watchtower flags weak, reused and breached passwords). The product, announced Oct 22, is “ 1Password for Agents. ” It fills in an approved login without exposing the password to the agent. On launch day several integrations were “rolling out” or “coming soon,” and 1Password says safeguards vary by integration. “Not sponsored” is his statement and cannot be checked from outside. Other reputable password managers exist.
Watch for fake breach emails such as one from “railway-alerts.com.”	PARTLY VERIFIED	The advice matches FTC guidance. Railway did suffer a real incident (official updates are at blog.railway.com). We found no record of “railway-alerts.com” as a live phishing domain; treat it as his illustration.

WHAT ACTUALLY HAPPENED THAT WEEK (CONFIRMED ITEMS)

- **PHP (“php2shell”)**: two unauthenticated remote-code-execution flaws in PHP itself; patches released Oct 21; CISA and NSA alerts the same day.
- **GitLab**: CVE-2026-110264, rated 10.0, affecting self-managed GitLab servers; patched Oct 21 (GitLab.com already fixed).
- **Railway**: unauthorized access to systems storing customers’ secret settings; the company says at most 1.85% of workspaces were potentially affected and asked earlier users to rotate secrets (Oct 22).
- **LiteLLM**: a compromised release (1.107.0) of a popular AI developer library was published on Oct 21 and stole credentials.
- **Zeabur**: a cloud host reported roughly 321,000 accounts and 3.2 million configuration records exposed in an Oct 14–15 breach, and announced it will shut down by Dec 31 (Cybernews, Oct 22).
- **eMudhra**: private keys for eight certificate authorities run by this Indian company turned out to be tiny numbers (one was the number 4); Chrome, Firefox, Apple and Microsoft blocked them Oct 17–20.
- **California student data**: ETS, a testing contractor for the state, began notifying families on Oct 16 of unauthorized copying of student information; Social Security numbers, financial information and parent information were not involved.
- **Quest Diagnostics**: unauthorized access to its Quantum lab-ordering system affected some patient records (disclosed Oct 22); Quest says it is not related to the PHP flaw.

Other items on the viral “12” list (Cairn, Ahold Delhaize, Onamae, Signal, NGINX) were not individually confirmed in our check.

UNVERIFIED

SECTION 4

04 WHAT THE VIDEO LEAVES OUT

Good advice can still carry blind spots. These are the ones a family should know.

THE HEADLINE IS HOTTER THAN THE FACTS

“The internet is being hacked” suggests one ongoing attack on ordinary people. What happened was a stack of disclosures and breaches, mostly in servers and developer tools. The PHP flaw is your web host’s job to patch; an app on your phone does not fix it.

LETTING AN AI AGENT CLICK THROUGH YOUR ACCOUNTS

Security groups such as OWASP rank “prompt injection” as a top risk for AI agents: hidden instructions in an email or web page can redirect an agent that is logged into your life. The video’s prompt rules are well intended, but they are only instructions to the AI. A plain checklist you walk through yourself is safer.

PASSKEYS ARE MISSING

CISA’s goal is “phishing-resistant” sign-in: passkeys or hardware security keys. Where your email, bank or church admin account offers a passkey, prefer it over SMS and over app codes.

NEVER GIVE ANYONE YOUR BANK LOGIN

Chase told Axios customers should not give their username and password to anyone. That includes AI assistants. Do not give an agent authority to move money or make purchases.

“ROTATE EVERY API KEY” IS FOR BUILDERS

This step applies to people who run apps or code, and especially to anyone affected by Railway, LiteLLM or Zeabur. Most families have no API keys and can skip it.

SCAMMERS WILL USE THIS NEWS

Expect emails, texts and calls that mention PHP, your bank, or “Black October” and demand you click, call, or read a code aloud. Real companies and agencies will not ask you to give a code to a caller.

SECTION 5

05 FAMILY PROTECTION CHECKLIST

An afternoon’s work for most households. Do it together, then pray over your home and get back to ordinary life.

START WITH THE “MASTER KEYS”

- ☐ Secure your **main email** first: it can reset every other account.
- ☐ Then your **bank, credit cards and phone carrier** account.
- ☐ Run Google’s **Security Checkup** (myaccount.google.com) or the Apple/Microsoft equivalent, and remove devices you don’t recognize.

APPS & DEVICES

- ☐ Remove apps and browser extensions you no longer use, including “Sign in with Google” connections.
- ☐ Turn on **automatic updates** for phones, computers and browsers.
- ☐ Think twice before connecting an AI assistant to email or banking. Never give one your bank password or the ability to move money.

MESSAGES & CALLS

- ☐ Family rule: **no one reads a code aloud** to anyone who calls.

PASSWORDS

- ☐ Use a reputable password manager (1Password, Bitwarden, Apple Passwords or Google Password Manager).
- ☐ Replace **reused** passwords, starting with email and banking.
- ☐ Check your email addresses at **haveibeenpwned.com**.

SIGN-IN PROTECTION

- ☐ Turn on a **passkey** wherever offered (strongest).
- ☐ Otherwise use an **authenticator app**, not text messages.
- ☐ Ask your carrier for a **port-out PIN / SIM lock** to block SIM swaps.
- ☐ Save your recovery codes somewhere safe and offline.

- ☐ Check the sender's real address and hover over links before clicking.
- ☐ When a message says "urgent," open the company's app or type its address yourself.
- ☐ Agree on a **family code word** for emergency calls (voice cloning is real).
- ☐ Talk with children and older parents about these scams; they are frequent targets.

FOR CHURCHES & MINISTRIES

- ☐ If your website runs on WordPress or other PHP software, **ask your host** whether PHP has been updated to a patched version.
- ☐ Update plugins and themes; remove unused admin accounts.
- ☐ Use passkeys or app-based two-factor for giving platforms, email and admin logins.
- ☐ Do not install "PHP fixer" tools from ads or unsolicited emails.

If you think you were hit

Change the password from a clean device, sign out all other sessions, and turn on stronger sign-in. Call your bank using the number on your card. For identity theft, use the federal recovery plan at [IdentityTheft.gov](https://www.identitytheft.gov). Report scams to the FTC at [ReportFraud.ftc.gov](https://www.reportfraud.ftc.gov). Never use a phone number or link from the suspicious message itself.

BOTTOM LINE

The week was serious, but the response for most families is simple: secure your email and bank, use unique passwords and stronger sign-in, update your devices, and refuse to act on panic. Be watchful, not fearful. "Unless the LORD guards the city, the watchman stays awake in vain" (Ps 127:1).

SECTION 6

06 SOURCES

All links accessed Oct 23, 2026. Research was gathered with a live-search research tool; sources 1, 3–5, 7, 9–18, 20–21, 24 and 30 were then opened and read by hand.

The video & creator

1. Peter Yang, "The Internet Is Being Hacked. 6 Things You Need To Do Now," YouTube, Oct 22, 2026. <https://www.youtube.com/watch?v=nXmLSq4aFBg>
2. Peter Yang on X, Oct 22, 2026 (agent alert post). <https://x.com/peteryang/status/2113299343855988843>

PHP & government guidance

3. CISA, "Critical Vulnerabilities in PHP Require Immediate Patching," Oct 21, 2026. <https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching>
4. NSA, "NSA Advisory: Critical Patches Recommended for PHP Vulnerabilities," Oct 21, 2026. <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4630238/>
5. Wiz Research, php2shell write-up, Oct 21, 2026. <https://www.wiz.io/blog/php2shell-php-rce>

6. The Register, Oct 21, 2026.
<https://www.theregister.com/security/2026/10/21/php-devs-publish-critical-bug-fix-as-site-owners-warned-pull-em-offline-if-youre-unpatched/5304519>

Banks & AI agents

7. Madison Mills, “Scoop: Unvetted AI agents are accessing U.S. bank accounts,” Axios, Oct 22, 2026. <https://www.axios.com/2026/10/22/ai-agents-banks-unauthorized-accounts-access>
8. Reuters, Oct 22, 2026. <https://www.reuters.com/legal/government/us-banks-detect-unauthorized-ai-agents-customer-accounts-axios-reports-2026-10-22/>
9. CBS News, Oct 23, 2026. <https://www.cbsnews.com/news/ai-agents-customer-bank-accounts-security/>

The week's other incidents

10. GitLab patch release 19.5.1, Oct 21, 2026.
<https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/>
11. Railway, preliminary incident report, Oct 22, 2026.
<https://blog.railway.com/p/preliminary-report-october-security-incident>
12. LiteLLM security incident, Oct 23, 2026.
<https://docs.litellm.ai/blog/security-incident-oct-21-2026-attack-chain>
13. Cybernews (Zeabur), Oct 22, 2026. <https://cybernews.com/news/zeabur-cloud-provider-shutdown-two-breaches-3-million-records/>
14. Internet Freedom Foundation (eMudhra), Oct 22, 2026.
<https://internetfreedom.in/a-private-key-with-the-value-4-iff-writes-to-emudhra-cert-in-and-meity-on-the-compromise-of-emudhras-certificate-authority-keys/>
15. California Department of Education, ETS notice.
<https://www.cde.ca.gov/nr/ne/yr26/yr26rel45.asp>
16. Quest Diagnostics, Quantum notice (updated Oct 23, 2026).
<https://www.questdiagnostics.com/links/quantum-notice>
17. The Guardian, Oct 23, 2026.
<https://www.theguardian.com/technology/2026/oct/23/cybersecurity-ai-hacking-php-vulnerability>

18. Matteo Wong, “Welcome to the Valley of Pain” (web title “The Safe Internet Is Shrinking”), The Atlantic, Oct 23, 2026.
<https://www.theatlantic.com/technology/2026/10/the-safe-internet-is-shrinking/689130/>
19. Forkast via Yahoo Tech (“Black October” label), Oct 23, 2026.
<https://tech.yahoo.com/cybersecurity/articles/black-october-disclosure-wave-label-023233848.html>

Sign-in security, tools & household help

20. CISA, Multifactor Authentication. <https://www.cisa.gov/MFA>; ranking of methods: [cisa.gov/.../require-multifactor-authentication](https://www.cisa.gov/.../require-multifactor-authentication)
21. CISA, “Implementing Phishing-Resistant MFA” fact sheet.
<https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>
22. NIST SP 800-63B-4, Digital Identity Guidelines, 2025.
<https://csrc.nist.gov/pubs/sp/800/63/b/4/final>
23. CISA, Cybersecurity Awareness Month.
<https://www.cisa.gov/cybersecurity-awareness-month>
24. 1Password, “Introducing 1Password for Agents,” Oct 22, 2026.
<https://1password.com/blog/1password-for-ai-agents>; pricing: <https://1password.com/pricing/personal>
25. OWASP, Top 10 for Agentic Applications (2026).
<https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/>
26. FTC, “Phishing scams can be hard to spot,” Dec 2024.
<https://consumer.ftc.gov/consumer-alerts/2024/12/phishing-scams-can-be-hard-to-spot>; FTC scams hub: <https://consumer.ftc.gov/scams>
27. IdentityTheft.gov. <https://www.identitytheft.gov/>; ReportFraud.ftc.gov. <https://reportfraud.ftc.gov/>
28. Have I Been Pwned. <https://haveibeenpwned.com/>
29. Google Account Help, third-party connections.
<https://support.google.com/accounts/answer/13533235>
30. Scripture quotations from the New King James Version® (NKJV), © 1982 Thomas Nelson. Used by permission. All rights reserved. Text checked at BibleGateway.com.

Could not verify

An official count of “12” incidents. Five items on the viral list (Cairn, Ahold Delhaize, Onamae, Signal, NGINX). “railway-alerts.com” as a live phishing domain. The contents of the creator’s screenshot and which agent triggered his alert. Whether the 1Password mention was unpaid (he says it was). Reuters blocked access; its points are covered by the Axios and CBS reports, which we read directly. Sources not opened by hand (2, 6, 8, 19, 22–23, 25–29) are cited as found by the research tool.