xmrwallet.com Victim Advisory

What To Do If You Lost Funds

PhishDestroy Research — February 2026

If You Used xmrwallet.com, Read This Carefully

xmrwallet.com has been confirmed as a fraudulent Monero wallet service that steals user funds. If you created a wallet or sent Monero through xmrwallet.com, your funds were likely stolen through one of two mechanisms:

1. **Private view key exfiltration** — Your private view key was captured via a hidden `session_key` parameter, allowing the operator to monitor your wallet balance in real time
2. **Transaction hijacking** — When you attempted to send Monero, the server replaced your transaction with a "sweep" that sent your entire balance to the operator's wallet

This was not your fault. The service was deliberately designed to appear legitimate while stealing funds behind the scenes.

Step 1: Confirm You Were Affected

Signs that your funds were stolen by xmrwallet.com:

- You sent Monero to someone, the transaction appeared "confirmed," but the recipient never received it
- Your wallet balance dropped to zero unexpectedly
- You noticed a transaction you did not initiate in your transaction history
- Your wallet shows a transaction with a hash you do not recognize
- You received an error or unusual response when attempting a transaction

If you still have funds in an xmrwallet.com wallet:

MOVE THEM IMMEDIATELY. Do not use xmrwallet.com to transfer funds. Instead:

1. Use your **seed phrase** (25-word mnemonic) to restore your wallet in a legitimate application (see Step 5 below)
2. Once restored in a safe wallet, immediately transfer all funds to a **brand new wallet** created in the safe application
3. The new wallet is necessary because xmrwallet.com has your private view key and can still monitor the original wallet

---

Step 2: Document Everything

Before taking any other action, preserve all evidence you have:

What to Save	How to Save It	Why It Matters
Transaction hashes (TX IDs)	Copy from xmrwallet.com transaction history, save to a text file	On-chain proof of theft
Screenshots of your wallet	Screenshot the balance, transaction history, and any error messages	Visual evidence for reports

Browser network logs	Open Developer Tools (F12) > Network tab, reproduce the issue, save HAR file	May contain session_key and raw_tx evidence
Email correspondence	Save any emails to/from xmrwallet.com support	Evidence of operator interaction
Dates and amounts	Write down when you deposited funds, amounts, and when you discovered the loss	Timeline for law enforcement
Your Monero address	The public address shown by xmrwallet.com	Identifies your wallet on the blockchain

Important: Do NOT share your seed phrase or private spend key with anyone, including law enforcement. They do not need it. Only share your public address and transaction hashes.

Step 3: Report to Law Enforcement

Cryptocurrency theft is a crime in most jurisdictions. File reports with:

United States

Agency	What to File	Link / Contact
FBI IC3	Internet Crime Complaint	https://www.ic3.gov
FTC	Consumer fraud report	https://reportfraud.ftc.gov
Secret Service	Financial crimes (losses over $100,000)	Contact local field office
State Attorney General	Consumer protection complaint	Varies by state

European Union

Agency	What to File	Link / Contact
Europol	Online fraud report	https://www.europol.europa.eu
National police	Criminal fraud complaint	Contact local cybercrime unit
Consumer protection	Cross-border fraud	https://ec.europa.eu/consumers

International

Agency	What to File	Link / Contact
Action Fraud (UK)	Cyber fraud report	https://www.actionfraud.police.uk
ACSC (Australia)	Cybercrime report	https://www.cyber.gov.au
Canadian Anti-Fraud Centre	Online fraud	https://www.antifraudcentre-centreantifraude.ca
Local police	Criminal theft report	Your local police station

When filing reports, include:

- The URL: xmrwallet.com

- Operator name: Nathalie Roy (GitHub: nathroy)
- The amount lost in XMR and approximate USD value at time of theft
- All transaction hashes
- The PhishDestroy Research report URL as supporting evidence

---

Step 4: Report to Industry Organizations

Help prevent others from becoming victims:

Platform	Action	Link
Google Safe Browsing	Report phishing/scam site	https://safebrowsing.google.com/safebrowsing/report_phish/
PhishTank	Submit phishing URL	https://www.phishtank.com
VirusTotal	Flag as malicious (already 6/93 detections)	https://www.virustotal.com
Domain registrar	File abuse complaint against xmrwallet.com	Identify registrar via WHOIS lookup
Hosting provider	File abuse complaint	Identify host via DNS lookup
Reddit r/Monero	Share your experience (warn others)	https://www.reddit.com/r/Monero
Monero community forums	Post warning	https://forum.getmonero.org

---

Step 5: Set Up a Legitimate Wallet

Transfer any remaining funds and conduct all future Monero transactions using only verified, reputable wallets:

Recommended Wallets

Wallet	Platform	Key Features	Download
Feather Wallet	Windows, macOS, Linux	Lightweight, open source, privacy-focused, highly recommended	https://featherwallet.org
Monero GUI Wallet	Windows, macOS, Linux	Official Monero Project wallet, full node option	https://getmonero.org/downloads
Cake Wallet	iOS, Android	Open source mobile wallet, user-friendly	https://cakewallet.com
MyMonero	Web, Desktop, Mobile	Created by Monero co-founder, established reputation	https://mymonero.com

Security Rules Going Forward

1. **Never use a web-only wallet** from an unknown provider — if it is not one of the wallets listed above, do not trust it
2. **Always verify download sources** — only download wallets from official websites, never from third-party links
3. **Store your seed phrase offline** — write it on paper, store in a secure location, never save digitally
4. **Never enter your seed phrase into a website** — legitimate wallets do not ask for this via a web browser
5. **Check community reputation** — before using any wallet, verify it on r/Monero and the official Monero website

---

Step 6: Understand the Recovery Reality

Honest assessment of fund recovery:

Scenario	Likelihood	Explanation
Direct recovery of stolen XMR	**Very low**	Monero transactions are irreversible by design; this privacy feature that protects users also protects thieves
Law enforcement seizure	**Low to moderate**	Requires identifying and locating the operator, legal proceedings, and the operator still holding identifiable assets
Civil lawsuit recovery	**Low to moderate**	Requires identifying the operator's real identity, jurisdiction, and seizable assets
Preventing future victims	**High**	Your reports directly contribute to getting the site flagged, blocked, and taken down

The most impactful action you can take is filing reports (Steps 3 and 4). Even if your funds cannot be recovered, your report:

- Adds to the body of evidence against the operator
- Helps law enforcement build a case
- Gets the site flagged by more security vendors (currently 6/93 on VirusTotal)
- Warns future potential victims through search results and security databases
- Supports domain suspension and hosting termination efforts

Frequently Asked Questions

Q: Can I get my Monero back? A: Unfortunately, Monero transactions are cryptographically irreversible. Once funds are swept to the operator's wallet, they cannot be "undone." Recovery depends entirely on law enforcement action against the operator.

Q: Is my seed phrase compromised? A: xmrwallet.com captured your **private view key** (which allows monitoring but not spending). However, because the service had full access to your wallet during use, you should treat the entire wallet as compromised. Create a new wallet in a legitimate application and transfer any remaining funds.

Q: Should I contact xmrwallet.com support? A: No. The "support" is operated by the same person stealing funds. Contacting them alerts the operator that you are aware of the theft and may prompt them to accelerate any remaining fund extraction. The hidden `/support_login.html` endpoint confirms that "support" is part of the theft infrastructure.

Q: Why does xmrwallet.com have Google trackers if it claims to be a privacy wallet? A: xmrwallet.com embeds 4 Google tracking mechanisms (Analytics, Tag Manager, Ads, Remarketing). No legitimate privacy wallet would include any advertising trackers. This further confirms the service is not what it claims to be — the trackers likely help the operator identify and profile victims.

Q: How long has this been going on? A: Evidence indicates xmrwallet.com has been stealing funds since at least **2016** — nearly a decade. The operator has stolen an estimated **$2,000,000+ USD** from **15+ documented victims**, with the true number likely much higher as many victims do not report.

Q: Why haven't they been shut down? A: The operator has actively evaded shutdown by deleting evidence (21+ GitHub issues), registering escape domains (xmrwallet.cc and xmrwallet.biz, both now suspended), and operating in jurisdictions with limited enforcement. Community reporting is the most effective tool — every report increases the likelihood of permanent disruption.

Need Help?

- **PhishDestroy Research:** https://phishdestroy.com — the organization that investigated and documented this fraud
- **Reddit r/Monero:** https://www.reddit.com/r/Monero — community support and scam awareness
- **Monero Official Site:** https://getmonero.org — verified wallet downloads and documentation

---

Advisory prepared by PhishDestroy Research — February 2026 Classification: PUBLIC — Share freely to protect potential victims Contact: https://phishdestroy.com