Here are the *top 3 security issues* Web3 retail consumers face when interacting with websites and dApps—tailored for Naoris Protocol's product development:

### 1. 🏴 Phishing & Transaction Phishing (e.g., Ice-Phishing, PTX-Phishing)

Consumers are frequently targeted through *phishing attacks designed for crypto*, which include:

* *Ice-phishing*: Scam websites or front-ends trick users into signing malicious transaction approvals—leading to full asset drains ([trustbytes.io][1], [learncrypto.com][2]).
* *Payload-based transaction phishing (PTX-Phish): Advanced scams that manipulate signed transaction payloads to redirect funds—accounting for **\$341.9 M* in losses from \~130,000 incidents in a recent 300-day study ([arxiv.org][3]).

These attacks are effective due to Web3's *non-reversible transactions* and users' tendency to approve without fully reading.

### 2. 🔐 Wallet and Private Key Compromise

User self-custody of private keys makes wallets both powerful and vulnerable:

* *Private key leaks*: Over \$408 M lost in H1 2024 from \~42 incidents due to exposed keys or wallet breaches ([trustbytes.io][1], [dev.to][4]).
* *End-user device malware or cloud compromises*: Examples include compromised employee or cloud systems leading to massive fund siphons ([learncrypto.com][2]).
* *Inadequate wallet safeguards*: Especially prevalent in mobile and browser wallets lacking strong protection like file encryption and deeplink security ([blockapex.io][5]).

### 3. 🧱 Smart Contract Vulnerabilities

Users face risks from flawed dApp or DeFi code:

* *Reentrancy, integer underflows, delegate-call bugs*: These have led to massive exploit losses, e.g. the infamous DAO hack and numerous DeFi incidents ([university.mitosis.org][6]).
* *Flash-loan/exploits & price manipulation*: Attackers leverage flash loans to manipulate prices and drain liquidity pools—hundreds of millions in losses, e.g. numerous BSC incidents ([borgsecurity.io][7]).
* *Access-control failures & protocol logic flaws*: Even minor code oversights—like improper permission checks—have cost users and protocols millions .

### 🚀 Why These Matter for Naoris Protocol

Threat	Impact on Retail Users	Opportunity for Naoris Product Innovation
Phishing / PTX Phishing	Users tricked into irreversible approvals → losing entire wallet balances	Build UI-level defenses: transaction payload alerts, approval simulations, whitelist matching, real-time scam detection
Wallet Security Risks	Key theft or device breaches lead to total asset loss	Offer wearable or multi-sig wrappers, encrypted vault features, session sandboxing, and secure backup helpers
Smart Contract Flaws	Funds lost or liquidity drained during interactions with dApps	Provide automated code audit tools, user-friendly risk warnings on dApps contracts, and real-time vetting dashboards

---

### ✅ Recommendation Summary

1. Implement *transaction-level anti-phishing tools* that highlight abnormal payloads or unknown destination contracts.
2. Provide *wallet-level hygiene enhancements* (sandboxed signing, auto-encryption, multisig barriers) to protect keys and funds.
3. Integrate *smart contract risk assessment* that labels or scores dApps for common vulnerabilities before interaction.

These three areas—phishing, wallet compromise, and contract code risk—represent the core security threats Web3 retail users face today. Let me know if you'd like me to expand on specific case studies, threat frequencies, or mitigation technologies!

[1]: https://www.trustbytes.io/blog/the-state-of-web3-security-in-2024-challenges-problems-types-of-hacks-and-industry-outlook?utm_source=chatgpt.com "TRUSTBYTES Site"
[2]: https://learncrypto.com/feed/articles/web3-scams-and-threats-web3-security-trends-to-watch-out-for?utm_source=chatgpt.com "Web3 Scams and Threats: Web3 Security Trends to Watch Out for"
[3]: https://arxiv.org/abs/2409.02386?utm_source=chatgpt.com "Dissecting Payload-based Transaction Phishing on Ethereum"
[4]: https://dev.to/nomzykush/web3-operational-security-lessons-from-the-bybit-14b-wallet-safe-hack-363i?utm_source=chatgpt.com "Web3 Operational Security: Lessons from the Bybit $1.4B Wallet Safe ..."

[5]: https://blockapex.io/web3-wallet-security-checklist/?utm_source=chatgpt.com "Web3 Wallet Security Checklist - BlockApex"
[6]:
https://university.mitosis.org/security-challenges-in-web3-lessons-learned-from-recent-hacks-and-exploits/?utm_source=chatgpt.com "Security Challenges in Web3: Lessons Learned from Recent Hacks and Exploits"
[7]: https://www.borgsecurity.io/blog/critical-web3-security-flaws?utm_source=chatgpt.com "10 Critical Web3 Security Flaws That Put Millions at Risk"