

# OPERATION AVALANCHE VICTIM CHECKLIST

Protect Your Crypto from Approval Phishing



- 1 **Stop sending money or crypto assets to the purported investment website**
- 2 **Stop communication immediately**
  - » Immediately stop responding to text messages, e-mails or calls with the people behind the purported investment website.
- 3 **Protect your crypto assets**
  - » Revoke any approval or consent you have given, knowingly or unknowingly, to a third party to access your crypto wallets. One tool you can use is Etherscan's Token Approval:
    1. Click on "Connect to Web3" button to link your wallet
    2. Review token approvals
    3. Revoke any unauthorized permissions.
    4. Note: A small transaction fee may apply.
  - » For added security, consider creating a new wallet and transferring the remaining crypto assets to it.
  - » Transfer crypto assets to a Canadian registered crypto trading platform.
- 4 **Protect your accounts**
  - » Change passwords on all accounts that have interacted with the purported investment website (crypto trading platforms, wallets, emails, etc.).
  - » Enable two-factor authentication (2FA) on all important accounts as additional security.
- 5 **Check for unauthorized transactions and notify financial institutions**
  - » Thoroughly check the transaction history of your wallet and your account at a Canadian registered crypto trading platform. Report any suspicious activity to the wallet provider and the crypto trading platform.
  - » Promptly contact your financial institution or payment provider if your bank accounts have been used, and request that all unauthorized transactions be stopped or cancelled.
- 6 **Document and report your situation**
  - » Gather all the information you have:
    - Record the sequence of events that led to your investment using the purported investment website.
    - Documents and receipts.
    - Copies of e-mails or text messages.
    - Proof of transfers.
    - Screenshots of the purported investment website.
  - » Report to your local securities regulator or police department or the Canadian Anti-Fraud Center.

## Additional tips

- Beware of collection services that promise to recover lost funds or crypto assets for a fee. These services are sometimes fraudulent.
- Carefully check the URL or application you use to access crypto asset services because fraudulent sites can look almost identical to legitimate ones.
- The URLs of legitimate websites generally begin with "https", indicating that the connection is secure.
- Use Canadian registered crypto trading platform to buy and sell crypto assets.