

WINVEST ACCOUNT SECURITY CHECKLIST

Investor Success Center • A Practical Checklist for Protecting Your WinVest Account & Cryptocurrency

Security starts with you. Use this checklist to review the most important steps for protecting your WinVest login, authentication information, cryptocurrency wallet, and transactions. Revisit it periodically—especially after changing a password, device, browser, phone, or wallet.

1. Secure Your WinVest Login

- Use a strong, unique password that you do not use on other websites.
- Do not share your WinVest password or PIN with anyone.
- If you believe your password or PIN may have been exposed, change it promptly through your account settings.
- Avoid saving your login information on shared or public computers.
- Always verify that you are visiting the official WinVest website before entering your login information.

2. Enable Two-Factor Authentication (2FA)

- Set up Google Authenticator or the currently supported authentication method in your WinVest Security Center.
- Keep the device used for authentication protected with a screen lock, PIN, fingerprint, or other device security.
- Never provide a current authenticator code to someone who contacts you unexpectedly.
- If you replace or lose your phone, follow the official WinVest account-recovery/support process rather than trusting unsolicited assistance.

3. Review Your WinVest Security Center

- Periodically review the browsers/devices and IP-address information shown in your WinVest Security Center.
- Look for activity you do not recognize.
- If something appears unfamiliar, secure your account and contact official WinVest Support.
- Review security settings again after changing devices, browsers, passwords, or authentication settings.

4. Protect Your Cryptocurrency Wallet

- Use a reputable cryptocurrency wallet or service that you understand how to operate.
- Protect the wallet with a strong password and available device-security features.
- Keep your recovery/seed phrase private and stored securely offline.
- Never email, text, photograph, or publicly store your recovery phrase unless you fully understand the security risks.
- Never give your private keys or recovery phrase to WinVest, a team member, support agent, or anyone else.

5. Verify Bitcoin Addresses Before Sending

- Copy and paste Bitcoin addresses whenever possible rather than typing them manually.
- Compare the beginning and ending characters of the pasted address with the intended address before sending.
- Confirm that you are using the correct cryptocurrency and network.
- For a new or unfamiliar destination, consider a small test transaction when practical.
- Remember that cryptocurrency transactions generally cannot be reversed once sent and confirmed.

6. Protect Your Withdrawal Wallet Address

- Confirm that the withdrawal wallet address saved in your WinVest account belongs to you and is correct.
- Recheck the address before requesting a withdrawal, especially if you recently changed wallets.
- Treat any unexpected change to your saved withdrawal information as a security concern.
- Do not change a wallet address simply because someone contacting you tells you to do so.

7. Watch for Phishing & Impersonation

- Be suspicious of messages claiming you must act immediately to prevent account loss or suspension.
- Do not trust a message solely because it uses the WinVest name, logo, or an employee's name.
- Be cautious with links received through email, Telegram, WhatsApp, social media, or private messages.
- Never send cryptocurrency to someone claiming they need it to 'verify,' 'unlock,' 'upgrade,' or 'recover' your account unless you independently confirm the request through official WinVest resources.
- When uncertain, go directly to WinVest through the official website rather than using a link supplied in a message.

8. Keep Your Devices Secure

- Keep your phone, computer, browser, and security software updated.
- Use a screen lock on devices that can access your WinVest account or cryptocurrency wallet.
- Avoid accessing financial or cryptocurrency accounts over unsecured public Wi-Fi when possible.
- Do not install unknown software, browser extensions, or remote-access applications at the request of an unsolicited contact.

9. If You Suspect a Security Problem

- Stop and do not send additional funds or disclose additional information.
- Change compromised passwords from a trusted device.
- Review your WinVest Security Center and wallet activity.
- Contact WinVest through its official Support Center when the issue involves your WinVest account.
- If your cryptocurrency wallet may be compromised, follow the wallet provider's official security/recovery guidance immediately.

Investor Success Center Tip: No legitimate reason exists for another person to know your wallet recovery phrase or private keys. Treat those credentials as the keys to your cryptocurrency. Anyone who obtains them may be able to control the assets in that wallet.

Periodic Security Review

Review Item	Date Checked
WinVest password / PIN	_____
Two-factor authentication	_____
Security Center devices / IP activity	_____
Withdrawal wallet address	_____
Wallet security / recovery phrase storage	_____
Phone / computer security updates	_____

Educational Use Only: This checklist provides general security guidance and is not a substitute for current official WinVest instructions or the security guidance of your wallet/provider. Platform features and procedures may change. Always refer to official WinVest resources for current account-security requirements and support procedures.