

道口證券网络安全及网上交易安全指引
DaoKou Securities Cybersecurity and Online Trading
Security Guidelines

1. 认识常见网络安全风险

Understanding Common Cybersecurity Risks

随着互联网及电子交易服务的普及，网络攻击与诈骗手段亦不断升级。不法分子可能通过伪造身份、仿冒网站、恶意程序或其他方式，窃取客户的个人资料、账户凭证及资金。为保障您的账户与资产安全，请提高网络安全意识，并留意以下常见风险。

With the growing popularity of the Internet and electronic trading services, cyberattacks and fraud methods are also constantly evolving. Criminals may steal clients' personal information, account credentials, and funds by impersonating identities, creating fake websites, using malicious programs, or other means. To protect your account and assets, please raise your cybersecurity awareness and pay attention to the following common risks.

1.1 网络钓鱼及虚假信息攻击

Phishing and False Information Attacks

网络钓鱼（Phishing）是指不法分子冒充银行、证券公司、政府部门、快递服务商或其他可信机构，通过电子邮件、短信、语音电话及即时通讯软件发送虚假信息，诱使受害者点击恶意链接、开启可疑附件，或在仿冒网站输入登录密码、一次性密码（OTP）、银行卡资料等敏感信息。

Phishing refers to criminals impersonating banks, securities firms, government departments, courier services, or other trusted institutions and sending false information through emails, SMS messages, voice calls, and instant messaging software to trick victims into clicking malicious links, opening suspicious attachments, or entering sensitive information such as login passwords, one-time passwords (OTPs), and bank card details on fake websites.

常见手法及可疑迹象包括：

Common tactics and suspicious signs include:

伪造发送者身份：发件人名称、电子邮件地址或网站域名与官方信息相似，但可能存在字母替换、额外字符或其他细微差异。

Forged sender identity: The sender name, email address, or website domain may be similar to official information but may contain letter substitutions, extra characters, or other subtle differences.

制造紧迫感：以账户异常、限时验证、账户即将冻结等理由，要求立即采取行动。

Creating a sense of urgency: Using reasons such as account anomalies, time-limited verification, or accounts about to be frozen to demand immediate action.

诱导提交资料：要求通过指定链接更新个人信息、验证账户或提供安全认证资料。

Inducing submission of information: Requesting updates to personal information, account verification, or provision of security authentication information through specified links.

传播可疑内容：通过不明附件、二维码或超链接，引导用户进入虚假网站或下载恶意程序。

Spreading suspicious content: Using unknown attachments, QR codes, or hyperlinks to guide users to fake websites or download malicious programs.

1.2. 网络诈骗及身份冒充

Online Fraud and Impersonation

诈骗分子可能利用社交媒体、即时通讯平台及虚假投资网站，针对个人资料、账户及资金实施诈骗，主要包括：

Fraudsters may use social media, instant messaging platforms, and fake investment websites to commit fraud targeting personal information, accounts, and funds, mainly including:

虚假投资及高回报骗局：以内幕消息、保证盈利、低风险高回报等说辞吸引投资者，将其引导至虚假交易平台，甚至通过长期建立信任的方式诱骗受害者投入资金，即俗称的“杀猪盘”。

Fake investment and high-return scams: Using claims such as inside information, guaranteed profits, or low-risk high returns to attract investors and direct them to fake trading platforms, or even building trust over a long period to trick victims into investing funds, commonly known as “pig-butcher scams.”

冒充机构或熟人：假扮证券公司或银行职员、客服人员、执法人员及亲友，以各种理由要求转账、汇款或提供密码及验证码。

Impersonating institutions or acquaintances: Pretending to be securities firm or bank staff, customer

service personnel, law enforcement officers, or relatives and friends, and asking for transfers, remittances, passwords, or verification codes under various pretexts.

假冒客户服务：谎称账户出现异常、交易失败或需要退款，诱导用户提供银行资料，或安装远程控制软件。

Fake customer service: Falsely claiming that an account is abnormal, a transaction has failed, or a refund is needed, and inducing users to provide bank information or install remote-control software.

虚假中奖及优惠活动：以抽奖、赠品、补贴等名义收集个人资料，或要求预先缴付手续费、保证金等款项。

Fake prizes and promotional offers: Collecting personal information under the guise of lotteries, gifts, or subsidies, or requiring advance payment of handling fees, deposits, or other amounts.

对于任何涉及资金转移、账户验证或提供敏感资料的要求，均应先通过官方渠道核实，不应仅凭对方提供的联系方式或相关证明作出判断。

For any request involving fund transfers, account verification, or provision of sensitive information, you should first verify it through official channels and should not make judgments solely based on contact details or proof provided by the other party.

1.3. 恶意软件及其他网络攻击

Malware and Other Cyberattacks

除钓鱼及诈骗外，客户亦应留意以下网络安全威胁：

In addition to phishing and fraud, clients should also pay attention to the following cybersecurity threats:

恶意软件（Malware）：包括病毒、木马及间谍软件，可能记录键盘输入、截取屏幕内容、窃取账户信息，甚至远程控制设备。

Malware: Including viruses, Trojans, and spyware, which may record keyboard input, capture screen contents, steal account information, or even remotely control devices.

勒索软件（Ransomware）：通过加密设备或系统中的文件，限制用户访问数据，并以恢复文件为条件索取赎金。

Ransomware: Encrypting files on devices or systems, restricting user access to data, and demanding

ransom in exchange for restoring files.

仿冒移动应用程序：伪装成官方交易应用程序，诱导用户输入登录凭证或其他敏感资料。

Fake mobile applications: Disguised as official trading applications to induce users to enter login credentials or other sensitive information.

公共无线网络风险：通过未加密或伪造的 Wi-Fi 网络实施中间人攻击，尝试截取或篡改通信内容。

Public wireless network risks: Conducting man-in-the-middle attacks through unencrypted or fake Wi-Fi networks, attempting to intercept or tamper with communications.

社会工程学攻击：利用社交媒体等公开信息了解目标对象的背景，再通过电话、信息或日常交流获取敏感资料，或编造具有针对性的诈骗情节。

Social engineering attacks: Using public information such as social media to understand a target's background, then obtaining sensitive information through phone calls, messages, or daily interactions, or fabricating targeted fraud scenarios.

2. 个人账户与设备安全管理

Personal Account and Device Security Management

妥善管理登录凭证、保持设备安全，并及时安装系统及软件更新，是降低网络风险的重要措施。

Properly managing login credentials, keeping devices secure, and promptly installing system and software updates are important measures for reducing cyber risks.

2.1. 设置安全且独立的登录密码

Set Secure and Unique Login Passwords

使用长度充足、难以猜测的密码，并结合字母、数字及特殊符号，以提高密码强度。

Use sufficiently long and difficult-to-guess passwords, combining letters, numbers, and special symbols to improve password strength.

避免使用姓名、生日、电话号码及其他容易被推测的个人信息。

Avoid using names, birthdays, phone numbers, and other personal information that can be easily guessed.

不同网站及网上服务应使用不同的密码，尤其应为网上投资及交易账户设置独立密码。

Use different passwords for different websites and online services, especially setting a separate password for online investment and trading accounts.

定期检查密码安全状况；如怀疑密码已泄露，应立即更改。对于长期未更新且存在风险的密码，可主动进行更换。

Regularly check password security; if you suspect a password has been leaked, change it immediately. For passwords that have not been updated for a long time and carry risks, proactively change them.

避免在浏览器中启用不安全的密码自动保存功能，亦不要将密码明文记录在电脑、手机或他人容易接触的位置。

Avoid enabling insecure password auto-save functions in browsers, and do not record passwords in plain text on computers, mobile phones, or locations easily accessible to others.

2.2. 严格保护密码及安全认证资料

Strictly Protect Passwords and Security Authentication Information

登录密码、一次性密码（OTP）及安全编码器所产生的认证信息均属于重要的安全凭证，不应向任何第三方透露或共享。

Login passwords, one-time passwords (OTPs), and authentication information generated by security tokens are all important security credentials and should not be disclosed or shared with any third party.

道口证券的职员或持牌代表不会要求客户向其提供网上交易登录密码。如有人声称代表道口证券，并要求客户提供密码或其他敏感认证资料，请勿予以配合，并应立即通过官方渠道向本公司核实。

DaoKou Securities' staff or licensed representatives will not ask clients to provide their online trading login passwords. If someone claims to represent DaoKou Securities and asks clients to provide passwords or other sensitive authentication information, do not cooperate and immediately verify with the Company through official channels.

如账户支持双重认证（Two-Factor Authentication, 2FA），建议启用相关功能，并妥善保管用于接收一次性密码或生成安全编码的设备及工具。切勿将认证设备交由他人使用，亦不应向他人透露收到的验证码。

If an account supports Two-Factor Authentication (2FA), it is recommended that you enable this function and properly keep the devices and tools used to receive one-time passwords or generate security codes. Never let others use authentication devices, and do not disclose received verification codes to others.

2.3. 加强电脑及移动设备防护

Strengthen Computer and Mobile Device Protection

请确保用于访问网上投资平台的电脑、手机及其他终端设备处于安全状态：

Please ensure that computers, mobile phones, and other terminal devices used to access online investment platforms are in a secure state:

安装可靠的防病毒、防间谍软件及防火墙，并定期更新病毒库和安全规则。

Install reliable antivirus, anti-spyware, and firewall software, and regularly update virus definitions and security rules.

及时升级操作系统、网络浏览器及交易应用程序，确保使用受支持且较新的版本。

Promptly upgrade operating systems, web browsers, and trading applications to ensure you use supported and relatively new versions.

为电脑及移动设备设置高强度解锁密码、生物识别验证（如适用）及自动锁屏功能。

Set strong unlock passwords, biometric verification (where applicable), and automatic screen lock functions for computers and mobile devices.

避免下载、开启或安装来源不明的文件、应用程序及软件更新。

Avoid downloading, opening, or installing files, applications, and software updates from unknown sources.

切勿随意浏览未经核实的网站，或点击可疑电子邮件、短信、即时通讯信息中的链接、附件及二维码。

Do not browse unverified websites arbitrarily, or click links, attachments, and QR codes in suspicious emails, SMS messages, or instant messages.

仅从官方应用商店或可信的官方渠道下载及更新应用程序。

Only download and update applications from official app stores or trusted official channels.

不应对移动设备进行“越狱”（jailbreak）或“Root”等可能削弱原有安全防护的操作。

Do not “jailbreak” mobile devices or perform “Root” operations that may weaken existing security protections.

在不需要时关闭 Wi-Fi、蓝牙及 NFC 等无线连接功能；连接无线网络时，应优先选择可信且经过加密保护的网路，并清理不再使用的自动连接设置。

Turn off wireless connection functions such as Wi-Fi, Bluetooth, and NFC when not needed; when connecting to wireless networks, prioritize trusted and encrypted networks, and clean up unused automatic connection settings.

2.4. 谨慎使用公共电脑及无线网络

Use Public Computers and Wireless Networks with Caution

请避免通过公共电脑、共享设备或未加密的公共 Wi-Fi 登录网上投资平台或进行交易。如确有需要，应优先选择可信、安全的网路环境，并避免在不受信任的设备上输入账户凭证。

Please avoid logging into online investment platforms or conducting transactions through public computers, shared devices, or unencrypted public Wi-Fi. If necessary, prioritize a trusted and secure network environment and avoid entering account credentials on untrusted devices.

使用网上交易系统时，应注意周围环境，防止他人窥视屏幕或密码。完成操作后，请务必安全退出账户，不要仅关闭浏览器窗口便离开设备。

When using an online trading system, pay attention to your surroundings to prevent others from viewing your screen or password. After completing operations, be sure to securely log out of the account; do not leave the device after merely closing the browser window.

2.5. 妥善处理个人资料及实体文件

Properly Handle Personal Information and Physical Documents

账户结单、交易记录及其他载有个人身份或账户资料的纸质文件，如处理不当，可能被不法分子用于身份冒充或其他欺诈活动。

Account statements, trading records, and other paper documents containing personal identity or account information may be used by criminals for identity impersonation or other fraudulent activities if handled

improperly.

请妥善保存相关文件；如确定不再需要，应先将载有个人资料的部分彻底粉碎或采用其他安全方式销毁，避免直接弃置于公共垃圾桶或其他容易被他人获取的地方。

Please keep such documents properly; if they are no longer needed, thoroughly shred the parts containing personal information first or destroy them in another secure manner. Avoid directly discarding them in public trash bins or other places easily accessible to others.

3. 网上投资平台及交易安全措施

Online Investment Platform and Trading Security Measures

进行网上投资及交易时，除保护账户凭证外，亦应注意登录方式、交易通知及账户活动，以便及时发现异常情况。

When conducting online investment and trading, in addition to protecting account credentials, you should also pay attention to login methods, transaction notifications, and account activity so that anomalies can be detected promptly.

3.1. 通过正确渠道访问交易平台

Access the Trading Platform Through the Correct Channels

请使用以下方式进入道口证券的网上投资平台：

Please use the following methods to enter DaoKou Securities' online investment platform:

直接输入经核实的官方网站网址；使用已确认无误的官方网页书签；通过官方应用商店下载的道口证券移动应用程序登录。

Directly enter the verified official website URL; use confirmed official webpage bookmarks; log in through the DaoKou Securities mobile application downloaded from an official app store.

切勿通过来历不明的电子邮件、即时通讯信息、网页弹出窗口或其他超链接进入交易登录页面，亦不要在未经核实的网站上提交密码及个人敏感资料。

Never enter the trading login page through unknown emails, instant messages, web pop-ups, or other hyperlinks, and do not submit passwords or sensitive personal information on unverified websites.

3.2. 留意登录过程中的异常情况

Watch for Anomalies During Login

登录及使用交易平台期间，请注意网页和系统操作是否出现异常，例如：

During login and use of the trading platform, please pay attention to whether the webpage and system operations show anomalies, such as:

突然弹出可疑窗口或跳转至陌生网站；要求提供与正常登录或交易无关的额外个人资料；页面显示异常，或系统提示与平常使用情况明显不符。

Sudden suspicious pop-ups or redirection to unfamiliar websites; requests for additional personal information unrelated to normal login or trading; abnormal page display, or system prompts clearly inconsistent with usual use.

如发现上述情况，应暂停操作，并通过官方渠道确认系统及账户状态。

If any of the above occurs, suspend operations and confirm the system and account status through official channels.

3.3. 启用双重认证及交易通知

Enable Two-Factor Authentication and Transaction Notifications

为加强账户访问控制，建议客户启用平台提供的双重认证（2FA）功能，并按照系统指引完成身份验证。

To strengthen account access control, clients are advised to enable the Two-Factor Authentication (2FA) function provided by the platform and complete identity verification according to system instructions.

同时，请确保已开启适用的股票交易确认通知，并及时查阅通过短信、应用程序推送或电子邮件发送的交易信息。请妥善保管用于接收认证信息的设备，避免他人未经授权使用。

At the same time, please ensure that applicable stock trading confirmation notifications are enabled, and promptly review transaction information sent via SMS, application push notifications, or email. Please properly keep devices used to receive authentication information and prevent unauthorized use by others.

3.4. 定期核对交易及账户记录

Regularly Check Transactions and Account Records

请及时查看交易系统发出的成交确认、电子邮件及其他交易通知，并定期核对账户持仓、交易记录及相关活动。

Please promptly review trade confirmations, emails, and other transaction notifications issued by the trading system, and regularly check account holdings, trading records, and related activities.

如发现任何未经授权的交易、异常登录或其他可疑账户活动，应立即联系道口证券，以便核实情况并采取适当措施。

If you discover any unauthorized transactions, abnormal logins, or other suspicious account activity, immediately contact DaoKou Securities so that the situation can be verified and appropriate measures can be taken.

4. 提高防骗意识及处理可疑情况

Raise Fraud Prevention Awareness and Handle Suspicious Situations

4.1. 对投资招揽及异常优惠保持警惕

Be Vigilant About Investment Solicitations and Unusual Offers

请审慎对待任何声称能够保证盈利、提供内幕消息或承诺高回报且风险极低的投资机会。对于通过社交媒体、即时通讯软件或陌生人主动联系而提供的投资建议，应特别谨慎。

Please be prudent about any investment opportunity claiming guaranteed profits, providing inside information, or promising high returns with very low risk. Be especially cautious about investment advice provided through social media, instant messaging software, or unsolicited contact by strangers.

作出投资决定前，请核实相关机构及人员是否具备适用的监管牌照，并通过监管机构的官方资料及相关机构的正式渠道进行查证。切勿仅因对方使用专业术语、展示盈利记录或提供看似真实的文件，便轻信其身份及投资承诺。

Before making investment decisions, please verify whether the relevant institutions and personnel hold applicable regulatory licences, and check through official information from regulators and formal channels of the relevant institutions. Do not lightly trust their identity and investment promises merely because they use professional jargon, show profit records, or provide seemingly authentic documents.

4.2. 核实涉及资金及敏感资料的要求

Verify Requests Involving Funds and Sensitive Information

如收到要求转账、汇款、修改账户资料、提供验证码或安装远程控制软件的电话、短信或即时通讯信息，请先暂停操作，并独立通过官方渠道核实。

If you receive phone calls, SMS messages, or instant messages requesting transfers, remittances, modification of account information, provision of verification codes, or installation of remote-control software, please pause the operation first and independently verify through official channels.

即使对方能够说出您的姓名、账户相关信息或其他个人资料，也不代表其身份真实。请勿使用可疑信息中提供的电话号码或链接作为唯一的核实方式。

Even if the other party can state your name, account-related information, or other personal data, this does not mean their identity is genuine. Do not use the phone number or link provided in suspicious messages as the only method of verification.

4.3. 发现异常时及时采取行动

Take Prompt Action When Anomalies Are Discovered

如怀疑自己已点击恶意链接、下载可疑程序、泄露密码或遭遇未经授权的交易，请立即：

If you suspect that you have clicked a malicious link, downloaded a suspicious program, leaked a password, or encountered unauthorized transactions, please immediately:

停止相关操作，不再输入任何密码、验证码或其他敏感信息。

Stop the relevant operations and no longer enter any passwords, verification codes, or other sensitive information.

如怀疑账户凭证已泄露，应尽快通过安全渠道更改密码，并在适用情况下采取账户保护措施。

If you suspect account credentials have been leaked, change passwords as soon as possible through secure channels and take account protection measures where applicable.

保存可疑信息、电子邮件、电话号码、网址及相关交易记录，以便后续调查。

Preserve suspicious messages, emails, phone numbers, URLs, and relevant transaction records for

subsequent investigation.

立即通过道口证券的官方联络渠道报告情况，并按照指引处理。

Immediately report the situation to DaoKou Securities through its official contact channels and handle it according to instructions.

如涉及资金损失或其他疑似违法行为，应视情况向相关银行、支付服务机构或执法部门报告。

If financial loss or other suspected illegal acts are involved, report to the relevant banks, payment service providers, or law enforcement authorities as appropriate.

请勿继续与可疑人士沟通，亦不要按照对方指示支付所谓的解冻费、保证金或其他款项。

Do not continue communicating with suspicious persons, and do not follow their instructions to pay so-called unfreezing fees, deposits, or other amounts.

5. 网络安全重点提示

Key Cybersecurity Reminders

为保障您的个人资料、账户及投资资产安全，请时刻谨记以下原则：

To protect your personal information, accounts, and investment assets, please always remember the following principles:

密码不外泄：不向任何人透露登录密码、一次性密码或安全认证资料。

Never disclose passwords: Do not disclose login passwords, one-time passwords, or security authentication information to anyone.

链接先核实：不随意点击可疑链接、附件或二维码，登录前仔细核对网址。

Verify links first: Do not casually click suspicious links, attachments, or QR codes, and carefully check the URL before logging in.

设备常更新：保持操作系统、浏览器、交易应用程序及安全软件处于更新状态。

Keep devices updated: Keep operating systems, browsers, trading applications, and security software in an updated state.

交易勤核对：及时查看交易通知，并定期检查账户活动及成交记录。

Check transactions frequently: Promptly review transaction notifications and regularly check account activity and trade records.

投资慎判断：对保证盈利、异常高回报及未经核实的投资招揽保持警惕。

Judge investments carefully: Be vigilant about guaranteed profits, unusual high returns, and unverified investment solicitations.

异常速报告：如发现可疑情况或怀疑账户受到影响，应立即停止操作并联系道口证券。

Report anomalies immediately: If you discover suspicious circumstances or suspect your account has been affected, immediately stop operations and contact DaoKou Securities.

网络安全需要客户与金融服务机构共同维护。道口证券建议您定期检查个人账户及设备的安全设置，持续提高网络风险防范意识，并通过官方渠道获取最新的安全提示。

Cybersecurity requires the joint efforts of clients and financial services institutions. DaoKou Securities recommends that you regularly check the security settings of your personal accounts and devices, continuously improve your awareness of cyber risk prevention, and obtain the latest security tips through official channels.

如发现任何可疑信息、异常账户活动或疑似网络诈骗，请立即通过道口证券官方渠道联络本公司核实。

If you discover any suspicious information, abnormal account activity, or suspected online fraud, please immediately contact the Company through DaoKou Securities' official channels for verification.

客戶網路安全意識測驗

Client Cybersecurity Awareness

Part A: Phishing, Fraud, and Suspicious Requests

第一部分：钓鱼、诈骗及可疑请求

1. Should you enter your online trading password after clicking a login link in an unexpected email or SMS?

收到来历不明的电子邮件或短信中的登录链接后，是否应输入网上交易密码？

Yes / No

2. Is it safe to share your one-time password (OTP) with someone who claims to be from Daokou Securities?

将一次性密码（OTP）告知自称道口证券职员的人是否安全？

Yes / No

3. Is it safe to click a QR code from an unknown source to log in to your trading account?

扫描来源不明的二维码登录交易账户是否安全？

Yes / No

4. If someone can tell you your name and account details, is that proof they are a genuine Daokou Securities employee?

如果有人能说出您的姓名及账户资料，是否证明他是道口证券的真正职员？

Yes / No

5. Should you install remote-control software on your device because someone claiming to be customer service asked you to?

自称客服的人要求您安装远程控制软件，您是否应照做？

Yes / No

6. Is an investment offer that guarantees high returns with very low risk likely to be legitimate?

保证高回报且风险极低的投资机会是否很可能是合法的？

Yes / No

7. Should you verify an investment company's regulatory licence through official channels before investing?

投资前是否应通过官方渠道核实投资公司的监管牌照？

Yes / No

8. Is it safe to continue communicating with a suspicious person to find out more before reporting?

在举报前继续与可疑人士沟通以了解更多，是否安全？

Yes / No

Part B: Passwords and Authentication

第二部分：密码及认证

9. Should you use the same password for your online trading account and your social media accounts?

网上交易账户与社交媒体账户是否应使用相同密码？

Yes / No

10. Is a password made up of your name and birthday considered strong?

由姓名和生日组成的密码是否算强度足够？

Yes / No

11. Should you enable two-factor authentication (2FA) if your account supports it?

如果账户支持双重认证（2FA），是否应启用？

Yes / No

12. Is it acceptable to let a family member use your authentication device or receive your verification codes?

让家人使用您的认证设备或接收您的验证码，是否可以接受？

Yes / No

13. Is it safe to save your trading password in plain text on your phone or computer?

将交易密码以明文形式保存在手机或电脑上是否安全？

Yes / No

Part C: Devices, Apps, and Networks

第三部分：设备、应用程序及网络

14. Should you install antivirus/anti-spyware and a firewall on devices used for online trading?

用于网上交易的设备是否应安装防病毒、防间谍软件及防火墙？

Yes / No

15. Is it safe to download a trading app from any third-party website if it looks official?

从任何第三方网站下载看似官方的交易应用程序是否安全？

Yes / No

16. Should you keep your operating system, browser, and trading app updated?

是否应保持操作系统、浏览器及交易应用程序更新？

Yes / No

17. Is public unencrypted Wi-Fi a safe place to log in to your investment account?

在未加密的公共 Wi-Fi 环境下登录投资账户是否安全？

Yes / No

18. Should you avoid using public or shared computers to log in to your investment account?

是否应避免使用公共或共享电脑登录投资账户？

Yes / No

19. Should you turn off Wi-Fi, Bluetooth, and NFC when you do not need them?

不需要时是否应关闭 Wi-Fi、蓝牙及 NFC？

Yes / No

20. Should you log out of your account after using an online trading platform, even if you are in a hurry?

使用网上交易平台后，即使赶时间，是否也应安全退出账户？

Yes / No

Part D: Account Monitoring and Reporting

第四部分：账户监察及报告

21. Should you check the website address carefully before entering your login credentials?

输入登录凭证前是否应仔细核对网址？

Yes / No

22. Should you review trade confirmations and account records regularly?

是否应定期查看成交确认及账户记录？

Yes / No

23. If you see an unauthorized transaction, should you wait until the end of the month before reporting it?

如发现未经授权的交易，是否应等到月底才报告？

Yes / No

24. Should you shred paper account statements before throwing them away?

丢弃纸质账户结单前是否应将其粉碎？

Yes / No

25. Should you report suspicious messages or account activity to Daokou Securities through official channels?

是否应通过官方渠道向道口证券举报可疑信息或账户活动？

Yes / No

Answer Key and Explanations

答案及解释

No.	Answer / 答案	Explanation / 解释
1	No / 否	Unexpected links may lead to phishing websites. Access the trading platform only through verified official channels. 来历不明的链接可能导向钓鱼网站。应仅通过经核实的官方渠道进入交易平台。
2	No / 否	Never share OTPs or passwords. Daokou Securities staff will not

No.	Answer / 答案	Explanation / 解释
		ask for your online trading login password. 切勿分享一次性密码或密码。道口证券职员不会要求您提供网上交易登录密码。
3	No / 否	Unknown QR codes can lead to fake websites or malware. 来源不明的二维码可能导向虚假网站或恶意程序。
4	No / 否	Criminals may know personal details. Always verify independently through official channels. 不法分子可能掌握个人资料。应始终通过官方渠道独立核实。
5	No / 否	Remote-control software can let fraudsters access your device and accounts. 远程控制软件可让诈骗分子访问您的设备及账户。
6	No / 否	Guaranteed high returns with low risk are a common fraud tactic. 保证高回报且低风险是常见诈骗手法。
7	Yes / 是	Always verify regulatory licences and institution details through official sources. 应始终通过官方资料核实监管牌照及机构资料。
8	No / 否	Stop communicating and report through official channels. 应停止沟通，并通过官方渠道举报。
9	No / 否	Use different passwords for different services, especially trading accounts. 不同服务应使用不同密码，尤其是交易账户。

No.	Answer / 答案	Explanation / 解釋
10	No / 否	Personal information such as names and birthdays is easy to guess. 姓名、生日等个人信息容易被推测。
11	Yes / 是	2FA adds an extra layer of account protection. 双重认证可加强账户保护。
12	No / 否	Never share authentication devices or verification codes. 切勿将认证设备或验证码交由他人使用。
13	No / 否	Passwords should not be stored in plain text where others may access them. 密码不应以明文形式保存在他人可接触的位置。
14	Yes / 是	Security software helps protect against malware and other threats. 安全软件有助防范恶意软件及其他威胁。
15	No / 否	Download apps only from official app stores or trusted official channels. 应仅从官方应用商店或可信官方渠道下载应用程序。
16	Yes / 是	Updates help fix security vulnerabilities. 更新有助修补安全漏洞。
17	No / 否	Public unencrypted Wi-Fi may be intercepted or fake. Avoid logging in to trading accounts through it. 公共未加密 Wi-Fi 可能被截取或伪造。应避免通过其登录交易账户。
18	Yes / 是	Public or shared computers may be unsafe. Avoid entering credentials on untrusted devices. 公共或共享电脑可能不安全。

No.	Answer / 答案	Explanation / 解释
		应避免在不受信任的设备上输入凭证。
19	Yes / 是	Turning off unused wireless functions reduces exposure to risks. 关闭不使用的无线功能可减少风险暴露。
20	Yes / 是	Always securely log out after using the platform. 使用平台后应始终安全退出账户。
21	Yes / 是	Check the URL carefully to avoid fake websites. 应仔细核对网址，避免进入虚假网站。
22	Yes / 是	Regular checks help detect unauthorized activity promptly. 定期核对有助及时发现未经授权的活动。
23	No / 否	Report unauthorized transactions immediately to Daokou Securities. 发现未经授权的交易应立即向道口证券报告。
24	Yes / 是	Shred documents containing personal or account information before disposal. 丢弃含个人或账户资料的文件前应先粉碎。
25	Yes / 是	Report suspicious messages or activity through official Daokou Securities channels. 应通过道口证券官方渠道举报可疑信息或活动。

Score Interpretation

分数说明

- **23–25 correct:** Excellent cybersecurity awareness.
23–25 题正确： 网络安全意识优秀。
- **20–22 correct:** Good awareness. Review the questions answered incorrectly.
20–22 题正确： 意识良好，请复习答错的题目。
- **15–19 correct:** Basic awareness. Re-read the DaoKou Securities Cybersecurity and Online Trading Security Guidelines.
15–19 题正确： 基本意识，建议重新阅读《道口证券网络安全及网上交易安全指引》。
- **Below 15 correct:** Please complete additional cybersecurity training and review the Guidelines carefully.
少于 15 题正确： 请完成额外网络安全培训，并仔细复习指引。