JACKSON®

BeSafe

Jackson® recognizes that information security is critical to maintaining the trust of our customers and financial professionals. To protect customer and business data, we've implemented an industry-standard information security program. We're committed to advancing our security to keep pace with evolving cyberthreat tactics to keep client and financial professional information safe.

Be aware: your email links to your identity

Account takeover (ATO) is a common cybersecurity threat we face today. A compromised account, like email, can give cybercriminals access to any account your email is connected to. They can reset your passwords and compromise your data on other websites.

Take the right steps to protect your identity and follow these best practices

1. **Keep your software updated.** Ensure your computer, smartphone and any other devices you use to access financial accounts are updated with the latest security patches and software updates.
2. **Create a unique password for financial and other websites.** Hackers use stolen passwords to check if you have also used them on other sites. Use a password manager to generate unique, complex passwords and keep them stored securely.
3. **Enable multi-factor authentication or two-factor authentication (MFA/2FA).** Passwords alone are weak. Hackers use a variety of tools that can crack weak passwords in minutes—sometimes even seconds. Enabling MFA or 2FA adds another layer of protection. In addition to a username and password, you may receive a code to a separate device, such as your phone or laptop.
4. **Recognize and report phishing.** Be cautious of emails, messages, or phone calls that ask for your personal information or direct you to log in to your account. Verify the sender's authenticity and avoid clicking on suspicious links or downloading attachments. Cybercriminals use phishing to spread malware or persuade you to share valuable information. If you weren't expecting an email, or if it looks suspicious, use an alternative communication method, like a phone number or separate email address to confirm the legitimacy of the email.

Financial professionals, be aware: your client's information may be compromised

By managing your client's funds, you may be the first target of a cybercriminal once their email account is compromised. To prevent and minimize the effects of fraudulent activity, it is up to financial professionals to pay close attention to client communications and requests.

- **Know your customer.** Be aware of your client's typical trade, fund transfer or disbursement activity.
- **Question changes to client instructions.** Look into any changes to or variations in account activity by contacting the associated parties through a method other than email.
- **Use a dual-step process for disbursements.** Confirm requests in a separate communication channel and verify that account information has not recently changed.
- **Confirm verbally.** Make a verbal confirmation using a phone number on file instead of one included in email communications.

Simple and powerful steps to keep data safe:

DEVICES AND PASSWORDS

- [ ] Install antivirus and antimalware software on all devices.
- [ ] Set antivirus and antimalware software and signatures to update automatically and run scans on a regular basis.
- [ ] Never share IDs, passwords or security questions.
- [ ] Ensure all applications, including your operating system, are updated. Enable automatic updates.
- [ ] Create strong and unique passwords for each account, and never reuse them. Generate and store passwords in a password manager.
- [ ] Enable MFA or 2FA whenever it's available.
- [ ] Create fake answers to security questions and store them in a password manager so you don't forget them.
- [ ] Secure mobile devices, such as phones and tablets, with passcodes or biometrics.
- [ ] Never use public or free Wi-Fi or kiosk computers unless on a virtual private network (VPN).

POLICIES AND PROCEDURES FOR FINANCIAL PROFESSIONALS

Financial professionals should take these steps to safeguard sensitive client information.

- [ ] Verify requests through multiple channels.
- [ ] Implement secondary approval for making banking information changes.
- [ ] Keep a call-back phone number on file to respond to a suspicious call.
- [ ] Require verbal confirmation of client requests using information on file.
- [ ] Use secure methods for sharing information, such as encrypted emails or secure file transfer services.
- [ ] Participate in ongoing cybersecurity training to stay informed about the latest threats and best practices. Encourage clients and colleagues to do the same.
- [ ] Review all email for potential phishing indicators, fraudulent activity and account compromise.
- [ ] Limit physical access to your devices and documents by using locks, secure storage for sensitive documents and be mindful of who has access to your work area.
- [ ] Ensure that all critical data is backed up regularly and stored securely. This can protect against data loss due to cyberattacks or hardware failures.

ADDITIONAL ONLINE RESOURCES

Cybersecurity and Infrastructure Security Agency (CISA)	Learn more
National Cybersecurity Alliance (NCA)	Learn more

Jackson is providing the above links solely for informational purposes and as a convenience to you. Jackson makes no representations concerning the content of the Third Party Sites. The provision of a link to a Third Party Site does not constitute an endorsement, authorization, recommendation, sponsorship, or affiliation by Jackson with respect to the Third Party Site.

BeSafe

Know how to report

If you or your clients notice suspicious activity, report it immediately. Staying vigilant and being proactive can help prevent fraud. Here are the ways to report:

- Visit our Contact Us page on jackson.com
- Call 877/565-2968

JACKSON®