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. Jackson is committed to advancing its security to keep pace with evolving cyberthreat tactics and 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 such as email can give cybercriminals access to any account your email is connected to and allows them to reset your passwords and compromise data on other websites.

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

1. **Create a unique password for financial and other websites.** Hackers use stolen passwords to check if you have also used them on other sites. Password managers such as LastPass, Dashlane, and 1Password can generate and keep unique passwords safe.
2. **Enable Multi-Factor Authentication (MFA).** Passwords by themselves are weak. Hackers use a variety of tools that can crack weak passwords in minutes, sometimes even seconds. Enabling MFA or two-factor authentication 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.
3. **Don't click on links or open email attachments.** Cybercriminals use fraudulent email, aka phishing email, to spread malware or persuade you to share valuable information. If you weren't expecting an email or it looks suspicious, use an alternative communication method, such as a phone number or separate email, to confirm the legitimacy of the email.

Financial professionals, be aware: Your client may be compromised

By managing your client's funds, you may be the first target of a cybercriminal once your client's 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.** Query any changes to or variations in account activity by contacting the associated parties through an avenue 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:

Cybercriminals are actively pursuing any vulnerability in network systems or procedures to steal information for profit. We all play a role in defusing cyberattacks and preventing them altogether. The checklist below gives you simple yet powerful steps to keep data safe.

COMPUTERS AND PASSWORDS	✓
Install antivirus/antimalware software on all machines	
Set antivirus/antimalware software and signatures to auto-update and run scans on a regular basis	
Never share IDs, passwords, or security questions	
Enable multi-factor authentication	
Create strong and unique passwords for all accounts	
Ensure security questions are distinct from anything revealed on social media and the internet	
Ensure your operating system and all applications are updated	
Enable firewall protection for all devices, including IoT (Internet of Things)	
Enable passcodes to secure mobile devices	
Exclusively use dedicated business Wi-Fi and systems	
Never use public or free Wi-Fi or kiosk computers unless on a virtual private network (VPN)	

POLICIES AND PROCEDURES	✓
Accept client instructions via a dual-step process only	
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	
Encrypt email or otherwise secure client communication	
Train all employees on cybersecurity and information security	
Review all email for potential phishing indicators, fraudulent activity, and account compromise	

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 800/873-5654

JACKSON®