

Cybersecurity best practices during the COVID-19 outbreak

Advisors are facing new cybersecurity challenges right now, from managing entirely remote workforces to avoiding COVID-related fraud. Below we've outlined important actions you can take immediately to protect firm and client data, along with best practices and resources you can leverage to strengthen your long-term cybersecurity strategy.

You can also visit our [Cybersecurity Resource Center](#) to access educational materials for your team members and clients, as well as in-depth resources including our [Cybersecurity Assessment](#), its accompanying [Cybersecurity Reference Guide](#), and a [Fraud Encyclopedia](#).

Quickly tighten security for remote workers

Make sure team members are keeping firm resources and client data safe while working remotely.

- **Home network security.** Change default administrator passwords on home wireless routers and then secure the Wi-Fi networks with strong security (WPA2 encryption) and a long, unique password.
- **System updates.** Ensure operating systems, software applications (including anti-virus), mobile apps, and device firmware are up to date on all computers and devices.
- **Technology use.** Only firm-approved software should be used to conduct business, and all web-based applications should be accessed exclusively through a secure remote connection to the firm's network.
- **Escalation process.** Ensure team members are aware of the process for reporting IT issues and potential cybersecurity or fraud incidents—and that your firm is prepared to quickly take appropriate actions.
- **Passwords.** Require the use of long, unique passwords, ideally through a firm-provided password manager.
- **Schwab's multi-factor authentication.** Activate Schwab's multi-factor authentication feature for all team members, especially those authorized to move money.
- **Firm policies.** Re-share—or draft—your firm's Acceptable Use Policy and/or Remote Access Policy.

Review firm practices

Check that the following safeguards are in place. Some of these measures can be implemented immediately, while others may require additional time and support from IT specialists.








- **Leverage digital tools.** Digital tools, such as Move Money with eAuthorization and digital account open, are always the fastest, most secure way to process client requests. When employees are working remotely, it's more important than ever to eliminate paper containing sensitive client information whenever possible. Using online tools reduces errors and delays, makes it easier to control access to client information, and provides greater transparency into work in process across your team.
- **Virtual Private Network.** Use a VPN across all remote systems to encrypt traffic and secure the connection to your firm's network.
- **Firm multi-factor authentication.** Utilize multi-factor authentication, such as a password and text, to control access to firm systems.
- **Remote copy and paste.** Disable the ability for firm data and content to be transferred from your network to an external network or device.
- **Secure web portal.** Protect data in transit, keeping sensitive information exchanged with clients and other professionals out of less secure communication channels, such as email.

Safeguard your clients and firm against fraud

Be sure that your team and clients are on the lookout for phishing and social engineering scams that aim to take advantage of the COVID-19 outbreak.

- **Email and text links.** Remind employees and clients to avoid fraudulent messages claiming to be from the World Health Organization, the Centers for Disease Control and Prevention, and other reputable organizations with links or downloads offering virus outbreak maps, information on stimulus payments or mask purchases, and donation opportunities. It's best to go directly to the trusted sites of government agencies and healthcare organizations.
- **Third-party providers.** Look out for fraudsters claiming to be from third-party providers your firm uses that are seeking login credentials or other information they can exploit for financial gain.
- **Senior and vulnerable investors.** The COVID-19 outbreak can be particularly stressful for seniors. Watch out for signs of diminished capacity, like confusion, as well as out-of-character behaviors or transactions from clients in this group. If fraud is suspected, contact Schwab immediately.
- **Transaction requests and activities.** Be on guard for scammers who pose as clients claiming a need for sudden or urgent funds related to the virus to pay for critical expenses or make charitable contributions. Directly verify all transaction request details with your clients by calling them at the phone number on record or via video chat.

Take advantage of trusted resources

- **Schwab's Cybersecurity Resource Center** . You'll find in-depth resources based on the National Institute of Standards and Technology (NIST) framework including:
 - [Cybersecurity Assessment](#)  and accompanying [Cybersecurity Reference Guide](#) 
 - [Fraud Encyclopedia](#) 
 - [Training for your team members](#) 
 - [Educational materials for your clients](#)
- **Schwab's multi-factor authentication.** Use the resources below to set up enhanced security measures for your staff when logging on to Schwab Advisor Center.
 - [Guide for users](#) 
 - [Guide for firm security administrators](#) 
- **StaySafeOnline.org.** Here you will find resources from the National Cyber Security Alliance including:
 - [COVID-19 Security Resource Library](#)
 - [Security Tips for Remote Workers](#)
- **SANS Institute.** This website offers resources including:
 - [A work-from-home deployment kit](#) with a one-page PDF to help team members work securely from home
 - [Information Security Policy Templates](#) to help you draft your own
- **Federal Trade Commission.** The FTC website includes guidance on how to [secure wireless networks](#).
- **Federal Deposit Insurance Corporation.** The FDIC provides resources to help recognize and avoid common cybersecurity threats.
- **Federal Bureau of Investigation.** The FBI has tips for staying safe as well as instructions on how to report suspected cybercrime and fraud.

Neither Charles Schwab & Co. Inc. nor any of its affiliates or employees makes any warranty, express or implied, or assumes any liability or responsibility for the accuracy, completeness, regulatory compliance, or usefulness of any information, tools, resources or process described within this document or in the Cybersecurity Resource Center, or represents that its use would protect against cybersecurity incidents, including but not limited to system breaches, compromise of firm security and/or improper access to confidential information.

Neither Charles Schwab & Co., Inc. nor any of its affiliates or employees is responsible for any damages or other harm that might occur as a result of, or in spite of, use of any information, tools, resources or processes described in the Cybersecurity Resource Center. Your firm alone is responsible for securing your systems and data, including compliance with all applicable laws, regulations, and regulatory guidance. References in the Cybersecurity Resource Center to any specific product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by Charles Schwab & Co. Inc. The Cybersecurity Resource Center contains links to content that is available on third-party websites. Please note that Schwab does not endorse these sites or the products and services you might find there.

For advisor use only. For general educational purposes.

Schwab does not provide legal, tax, or compliance advice. Consult professionals in these fields to address your specific circumstance.

©2020 Charles Schwab & Co., Inc. Member [SIPC](#). All rights reserved. Schwab Advisor Services™ serves independent investment advisors and includes the custody, trading, and support services of Schwab. Independent investment advisors are not owned by, affiliated with, or supervised by Schwab.

TWI (0420-0J01) MKT110862-00 (04/20)



Own your tomorrow.