charles SCHWAB

Advisor Services

# Your top 10 cybercrime questions answered

Cybersecurity and fraud are top of mind for advisors. We recently hosted several webcasts to help advisors understand current trends and learn ways they can protect their firm and clients. Below, we've summarized the top 10 questions we heard, along with answers and supporting resources.

## Protecting and educating clients

1. Our firm has a very strict policy requiring each employee to verify any wire or money movement requests directly with the client before we process them, especially requests made through email. We want to ensure transactions are as secure as possible. Are there additional guidelines or steps we can take, beyond simply calling the client at the phone number we have on file, that can help me feel more confident about the verification process?

   **Answer:** Speaking directly to your client is absolutely necessary, but it may not be realistic to rely on your team to accurately recognize the voice of each client. You may want to consider using additional safeguards, such as a verbal passcode established ahead of time between your firm and your client.

   Some firms also use video calling technology, such as Skype or FaceTime, to perform client verifications. In the case of a one-time wire request, consider using our electronic authorization tools, which provide a more secure channel for getting your client's approval of the wire.

2. We try to educate clients about the topic of cybercrime, but it can be overwhelming and even scary to them. Do you have any recommendations on the best approach for educating clients?

   **Answer:** With mainstream news sources reporting frequently on cybercrime, it's understandable that your clients may be overwhelmed. It might be helpful to start by sharing your firm's commitment to safeguarding their information and assets and then describing examples of the policies and procedures your firm has in place. That will give you the opportunity to explain why you will always verify any email-based requests via a phone call, and why you may need to probe more deeply into any unusual or potentially unsafe requests they make. Finally, you can highlight Schwab's commitment to safeguarding their assets and information, and help them access the SchwabSafe® web page. SchwabSafe contains important information, including a description of how we protect accounts at Schwab, what your clients can do to keep their information safe, and the Schwab Security Guarantee.

3. What exactly does the Schwab Security Guarantee cover?

   **Answer:** We want your clients to have the highest level of confidence when they do business with Schwab, so we offer them this simple guarantee: **Schwab will cover 100% of any losses in a client's Schwab accounts due to unauthorized activity.** However, keep in mind that transactions initiated by people who have been granted permission to act on behalf of an account holder, such as an investment advisor, are considered authorized and are not covered.

   For complete details, log in to the Schwab Advisor Center and visit the Online Security page to read the Schwab Security Guarantee.

## Safeguarding data and assets

4. Is it safe for me or my team to use public Wi-Fi connections, such as at an airport, restaurant, or hotel, to conduct business when we are on the road?

   **Answer:** Your information may be vulnerable when you log in via an unsecured wireless network, whether at home or in a public area. Some wireless networks in public areas are open, with no security in place, making it easier for individuals to access and use these networks. Do not use a wireless network when you aren't certain that the person or company responsible for the network is trustworthy. An alternative may be to create a personal Wi-Fi hotspot to connect your laptop to your mobile phone's cellular signal. Contact your cell phone carrier for information. For additional tips about keeping secure while traveling, log in to Schwab Advisor Center to see SchwabSafe Travel Tips for Your Employees.

5. We all rely on passwords to control access and protect our information. Can you provide any guidelines or policies around passwords that we should implement at our firm and recommend to our clients?

   **Answer:** First and foremost, you and your team should always keep your login IDs and passwords confidential. Never write them down or share them among members of your staff. Similarly, never use sensitive information as part of your login ID or password, and create strong passwords that contain at least eight characters, with a combination of upper- and lowercase letters, numbers, and symbols. Create different passwords for each website and change them periodically. For additional information, log in to Schwab Advisor Center to see Safeguard Your Firm and Your Clients' Information.

6. It's hard to remember all the passwords we rely on across the various systems we use. Are password manager programs safe? If so, is there one particular solution that you recommend?

   **Answer:** One of the best ways you, your staff, and your clients can minimize risk and make it more difficult for criminals is to create complex passwords, update them periodically, and use a different user ID and password for each site.

   To make it easier to adhere to the guidelines above, some people use a password manager program. While it is possible for a master password to be compromised, many users choose this solution because there is only one password to remember. When using a password manager, each password is associated with one URL. Therefore, if a user accidentally clicks a link leading to a phishing site that looks legitimate, the password manager will not automatically enter a password for a URL that the user has not previously visited.

## Safe email practices

7. My clients prefer to conduct much of their business through email. If I use a secure service, like Google's Gmail, can I send sensitive information and accept things like wire requests through this channel?

   **Answer:** No matter which email system you use, we recommend that you do not conduct business or send personal, non-public information via email.

8. What are the key first steps when we suspect an email account has been hacked or otherwise compromised?

   **Answer:** Whether the email account that you suspect has been compromised is yours or your client's, time is of the essence: The sooner the issue is reported, the greater the likelihood of a potential recovery. However, even when you act quickly, there are never any guarantees. As an advisor, you should follow your internal procedures and immediately report unauthorized transactions to Schwab. You can also remind clients of the Schwab Security Guarantee. Recommend that your client run an antivirus/antispyware system scan, change passwords and email addresses, visit ftc.gov (search "identity theft"), and call the Schwab Alliance team to request a verbal password and/or security token. Log in to Schwab Advisor Center and read Preventing Fraud: Three Steps to Defend Your Firm and Your Clients to learn more.

## How Schwab protects your information and assets

9. We know that Schwab works proactively to identify fraud, including searching through a variety of sites and the so-called "dark web" to see if any advisor or end-client information is up for sale (Social Security numbers and other non-public information). Can you tell us more about your measures and procedures if you find that a client's information is being sold?

   **Answer:** We have a strong culture of risk management, and we ensure client accounts at Schwab are protected in multiple ways. We have designed and implemented a security program that knits together complementary tools, controls, and technologies to protect client accounts and data.

   We continuously monitor our systems and use vendors to monitor external sites to constantly adapt our own detection methodologies to detect potential client account compromises. If we determine a client's information appears to have been compromised, Schwab's response can vary from enhanced monitoring of the client's account to notifying the client immediately, based on the level of certainty that the client's accounts have been compromised. We also work collaboratively with government agencies, law enforcement, and other financial services firms to address potential threats and criminal activity.

Like other firms, we do not publicize the details of our behind-the-scenes security measures and practices, in order to make it more difficult for fraudsters to gain an edge by understanding the tools and techniques we apply.

10. With Schwab and other firms implementing solutions that rely on authentication through mobile phones, and now with news that fraudsters are targeting these phones with their hacks, should we be concerned?

    **Answer:** As technology becomes more sophisticated, fraudsters consistently look for the path of least resistance. Schwab works closely with law enforcement, other financial services firms, and security firms to adapt our detection technology as the threats change. If a criminal gains possession of a mobile device, whether it's in their physical possession or infected with malware or a virus, they may be able to view the client's email and other confidential information stored on the device. We also are now seeing phone numbers being forwarded so that when you call to verify a wire request, the fraudster answers the phone. This is why we suggest that when directly verifying transactions with clients, you include questions to which only your client would likely know the answers. You might also want to establish a password with your client, use video technology such as Skype or FaceTime to confirm your client's identity, or use electronic authorization to initiate a wire with your client, which incorporates security safeguards.

## Learn more

Below are resources that can help you enhance and keep abreast of current trends. We also encourage you to keep an eye on Schwab Advisor Center, as we will continue to add additional resources.

### Resources for you

Visit the Resources for you and your clients section of the Cybersecurity Resource Center. Here you will find actionable information and valuable tools to help you protect your clients and firm. It includes best practices, educational materials (including webcast replays), and sample talking points for communicating with clients. You'll also find updates on the latest fraud trends.

Review the information and resources available on industry and government sites, including:

- Federal Bureau of Investigation – Cybercrime (fbi.gov/about-us/investigate/cyber)
- FBI Internet Crime Complaint Center (ic3.gov/complaint/default.aspx)
- Federal Trade Commission – Privacy & Identity (consumer.ftc.gov/topics/privacy-identity)

### Resources for your clients

The Client Learning Center at content.schwab.com/learningcenter is a dedicated page where your clients can learn more about how you and Schwab work together to serve them. They'll find useful tips, including ways to protect their information and step-by-step guides for opening and servicing their accounts. They can also read about the Schwab Security Guarantee, which is designed to address concerns about online data security threats from non-trusted third parties.



Updated: May 2017