
Protect yourself against phishing.
Identify and report malicious activity.
charles SCHWAB
Own your tomorrow®

What is phishing?

Phishing is one of the most common forms of fraud, and it's essential to know how it works and how to protect yourself. In phishing attacks, criminals "bait" individuals into giving up valuable sensitive information or access to systems and devices. They do this by using deceptive tactics that may involve sending seemingly trustworthy communications or making phone calls that appear legitimate.

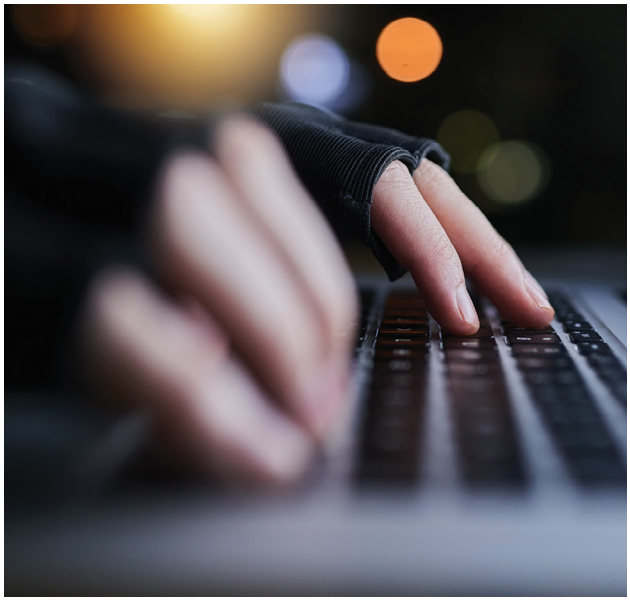
Phishing efforts use a variety of communication methods and techniques, including:

- Email
- Phone calls
- SMS texts
- Advertisements
- Social media
- Websites

The sender's identity is often imitated or masked, so recipients believe it's safe to disclose sensitive information such as:

- Usernames
- Passwords
- Social Security numbers
- Account numbers

What is phishing? *(continued)*



In some cases, phishing emails include links or attachments. Clicking on these links or opening the attachments may unknowingly install harmful software. This can lead to cybercriminals gaining access to your device and your information.

Criminals typically use information they obtain via phishing to commit identity theft and fraud; however, the fraud may not occur immediately. Often the perpetrators wait weeks or months for a favorable opportunity, or they may sell the information to other criminals.

Phishing attempts may also be deployed on social media platforms, broadening their reach, using:

- Fraudulent advertisements
- Friend requests
- Sharing posts and other tactics

What's the difference between a spam email and a phishing attempt?

Spam, sometimes referred to as junk mail, is typically an email solicitation intended to persuade the recipient to purchase goods or services. While some of these communications are misleading, the sender's desired outcome isn't always malicious.

Phishing, on the other hand, is a fraudulent attempt to obtain sensitive information or damage your computer. Both types of emails may look similar, making it difficult to distinguish between them. Given this, it's best not to click links or open attachments included with either type of email.

Still another tactic used is to send emails that appear to be spam, and include the option to click 'Unsubscribe' links to prevent future unwanted emails. In these instances, the 'Unsubscribe' links may be malicious.

Mark these emails as spam or junk, if your email provider supports this functionality, and delete them.

Tips to protect against phishing

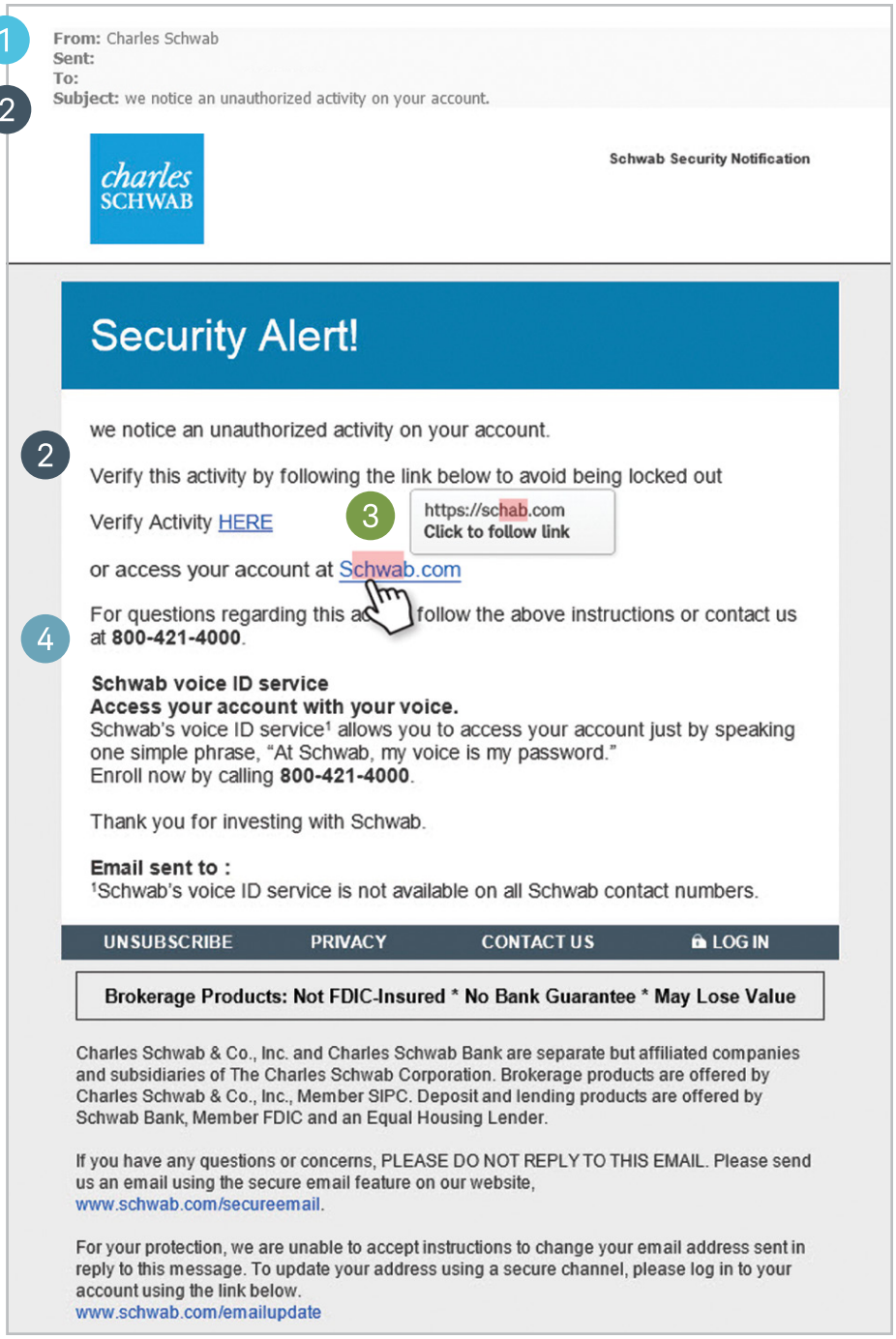
- Don't let your guard down when you receive emails from well-known companies, particularly financial institutions. Criminals often mimic emails from these companies to appear legitimate.
- Do not click on links or attachments included in unrecognized or suspicious emails or texts. If you do, never enter your username and password.
- Hover over links to reveal the website's URL and see where the link really goes. Do not click on links that don't match the sender or don't match what you expect to see:

Look for:	Example:
Slight alterations to the URL	**Scwab.com** or **Schab.com**
URLs that have the expected name embedded	**Schwab.fraudster.com** (note: the real domain is before the '.com')
URLs that are completely different from what you would expect to see	**Fraudster.com**

- Be cautious of emails with grayed out "CC:" and "To:" lines; these may indicate the email was sent to a mass distribution list.
- Check the sender's domain name in the email address (**john.doe@schwab.com**) to ensure it matches what you'd expect to see.
- Use spam filters and ad blockers to help reduce unwanted or potentially harmful communications. Additionally, install reputable antivirus software to provide protection against malware and viruses.
- Maintain separate email accounts with different login credentials: one for personal or financial email communications, and another for more public interactions, like mailing lists and businesses that require email addresses. This separation can help minimize the risk of mixing important emails with phishing attempts or spam.
- Enable two-factor verification to strengthen your account security. This requires a second form of verification, such as a unique PIN sent via text, email, or call, adding an extra layer of protection even if your credentials are compromised.
- Look for clues within emails such as errors in grammar, capitalization, or spelling; mismatched fonts; and incorrect information such as wrong phone numbers.
- Be wary of generic salutations that don't address you directly. For instance, emails that begin with 'Dear Customer' or 'Dear User' instead of your name may be phishing attempts.

Anatomy of a phish

Criminals often imitate emails that appear to be from financial institutions. Below is an example of a phishing attempt that appears to be from Schwab. There are several red flags that indicate this is not an actual communication from Schwab:



1 **From:** Charles Schwab
Sent:
To:
2 **Subject:** we notice an unauthorized activity on your account.

charles SCHWAB

Schwab Security Notification

Security Alert!

2 we notice an unauthorized activity on your account.

Verify this activity by following the link below to avoid being locked out

Verify Activity HERE 3 https://schab.com Click to follow link

or access your account at Schwab.com

4 For questions regarding this ac follow the above instructions or contact us at **800-421-4000**.

Schwab voice ID service
Access your account with your voice.
Schwab's voice ID service[1] allows you to access your account just by speaking one simple phrase, "At Schwab, my voice is my password."
Enroll now by calling **800-421-4000**.

Thank you for investing with Schwab.

Email sent to :
[1]Schwab's voice ID service is not available on all Schwab contact numbers.

UNSUBSCRIBE PRIVACY CONTACT US LOG IN

Brokerage Products: Not FDIC-Insured * No Bank Guarantee * May Lose Value

Charles Schwab & Co., Inc. and Charles Schwab Bank are separate but affiliated companies and subsidiaries of The Charles Schwab Corporation. Brokerage products are offered by Charles Schwab & Co., Inc., Member SIPC. Deposit and lending products are offered by Schwab Bank, Member FDIC and an Equal Housing Lender.

If you have any questions or concerns, PLEASE DO NOT REPLY TO THIS EMAIL. Please send us an email using the secure email feature on our website, www.schwab.com/secureemail.

For your protection, we are unable to accept instructions to change your email address sent in reply to this message. To update your address using a secure channel, please log in to your account using the link below.
www.schwab.com/emailupdate

1 When you hover over Charles Schwab, you see **fraudster@criminal.com**

2 Grammar, spelling, capitalization, or other language clues

3 When you hover over links, it reveals the URL **https://schab.com**

4 Lists an invalid contact number (Schwab's number is **800-435-4000**)

How Schwab works with you

In the course of servicing your account, Schwab may reach out to you using:

- Phone calls to confirm money movements or other transactions. These phone calls will request information so that we can verify we're actually speaking to you. If you have concerns about the legitimacy of the call, disconnect and dial **1-800-435-4000** to speak with a Schwab representative.
- Emails with:
  - Notification of recent account changes or transactions
  - Alerts that new documents are available, such as statements, trade confirmations, and tax forms
- Calls or texts to validate unknown ATM withdrawals.

Schwab will not:

- Ask you to disclose your Visa® debit card PIN
- Ask you to disclose your **Schwab.com** username and password (aside from logging in to **Schwab.com**)
- Ask you to provide personal information by email

If you're ever unsure that a call, text, or email is from Schwab, contact us directly to validate the request by:

- Logging on to **Schwab.com**
- Calling **1-800-435-4000**
- Calling the phone number on the back of your Visa® debit or credit card for bank inquiries

What to do if you suspect phishing

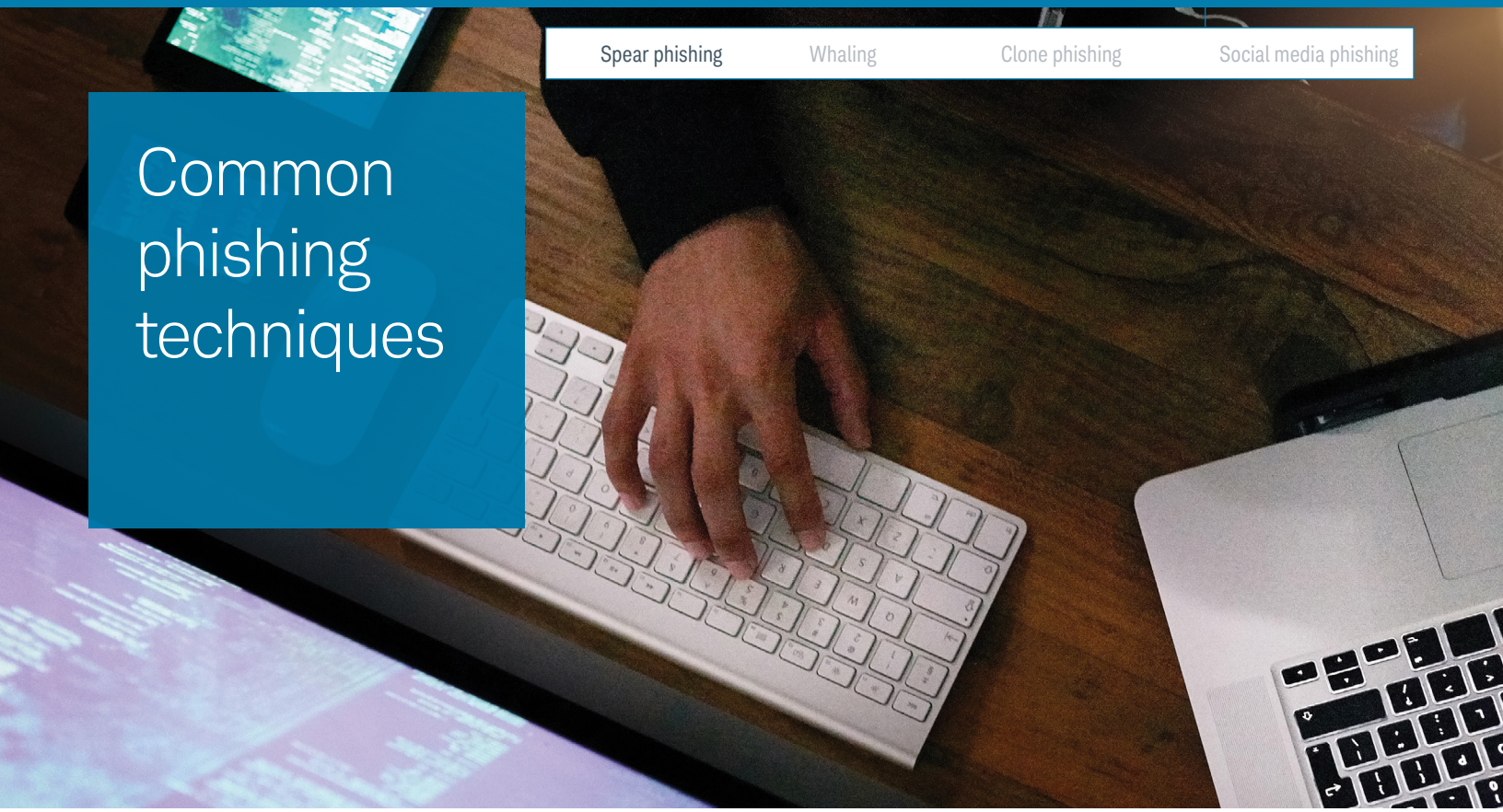
If you're suspicious about an email that appears to have come from Schwab, forward it to **phishing@schwab.com**.

If you ever doubt the authenticity of an email, or have provided your Schwab credentials after clicking a link from an email, call us at **1-800-435-4000**.

The Federal Trade Commission provides several external resources you can use to learn more about identity theft and how to report phishing attempts such as:

- File a report with the Federal Trade Commission at **FTC.gov/complaint**.
- Visit **identitytheft.gov** for steps you can take if you become a victim of identity theft.
- Report the phishing email to the Anti-Phishing Working Group at **reportphishing@apwg.org**.
- Notify the financial institution that was impersonated.

The FTC may update its resources periodically, so check **FTC.gov** for the most recent resources and directions.



Common phishing techniques

Spear phishing

What is it?

Individuals receive communications that may appear to be from a business or website they use—or even a family member or person the recipient knows. The goal is to lure the recipient into clicking on a malicious link or attachment and providing personal information.

For example, an individual may receive an email that appears to be from a financial institution they use, asking the recipient to click on a link under the guise of needing updated information or help to resolve a security or account issue.

Protect yourself

Refer to the general tips about preventing and detecting phishing attempts on page 4. Be cautious of communications via text, phone call, or email, even if they appear to be from a trustworthy source.

Whaling

What is it?

Whaling targets high-profile, high-net-worth individuals such as celebrities, corporate executives, or politicians. Criminals often use public information regarding the person's company or other affiliations, as well as information found on social media, to craft the phishing communication. The criminal may be trying to access the individual's assets or obtain sensitive information they might have access to due to their position.

Whaling can also be used to gain access to a high-profile individual's email account so the fraudsters can email employees at a business asking them to perform a task, such as transferring funds or disclosing highly sensitive information. This tactic is known as Business Email Compromise (BEC).

Protect yourself

Refer to the general tips about preventing and detecting phishing attempts on page 4 and limit the amount of private information you provide on social media.

Tips for business owners:

- Provide security awareness training for employees at all levels of your business, including senior leadership. Consider conducting phishing simulations.
- Administer an authorized simulated cyber-attack within the company.
- Establish and enforce effective verification procedures for money movement or the sharing of sensitive information.

Clone phishing

What is it?

Criminals copy a legitimate email communication an individual has already received and resend it with malicious links or attachments. The email address may look like it's from the original sender, but the address is "spoofed" (example: **Jane.D0e@phishing.com** vs. **Jane.Doe@phishing.com**).

Clone fishing can be one of the more successful phishing tactics since it uses communication or transactions the recipient is familiar with.

Protect yourself

Refer to the general tips about preventing and detecting phishing attempts on page 4. Remember that even if an email looks like one you've already received, it may be a phishing attempt.

Social media phishing

What is it?

Cyber criminals use several tactics to phish social media users, including:

- Fake friend profiles: Criminals duplicate others' profiles and send friend requests to the individual's contacts to lure them into accepting the request.
- Malicious links: Videos, sweepstakes, ads, chain letters, or other media are posted in the newsfeed. If clicked, a user could get a virus or be sent to a fake website.
- Social engineering: Criminals use information on a user's profile to either impersonate them or create a spear phishing attempt.
- Customer support: Fraudsters posing as customer support may ask their target to supply credentials to resolve an issue.
- Fake direct messages: Direct message requests with malicious links or attachments are sent via social media.

Protect yourself

Refer to the general tips about preventing and detecting phishing attempts on page 4. In addition:

- Review and update your security settings and privacy settings to limit information that can be accessed publicly.
- Close old social media accounts.
- Do not accept friend requests from people you don't know or repeat requests from people to whom you're already connected.
- Enable two-factor authentication and use strong and unique passwords for your social media accounts.
- Use caution when deciding what to click on.