



# Fraud Protection

Help you Recognize and Avoid Phishing Scams

## What is Email fraud?

Internet scammers casting about for people's financial information have a new way to lure unsuspecting victims: They go "phishing". Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

## How does it work?

Phishers send an email, SMS or pop-up message that claims to be from a business or organization that you deal with such as your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't. The purpose of the bogus site is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

If you get an email, SMS or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.

Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, such as a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

Be wary of look-alike websites. Fraudsters can develop websites that look very similar to CTBC's website, with the purpose of deceiving you into entering your username and password. The URL's in these websites resemble our legitimate URL very closely. However, fraud websites' URLs are always a little different, such as <https://www.ctbc-bank-usa.com> (notice the dashes in the URL). Any URL that doesn't match CTBC's official website URL should not be trusted.

## How to protect yourself against email fraud?

- If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.
- Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Use anti-virus software and keep it up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.
- A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Finally, your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that hackers or phishers could exploit.
- Be cautious about opening any attachment or downloading any files from emails you received, regardless of who sent them.

## Where to report the email fraud?

Report suspicious activity to the FTC. If you get spam that is phishing for information, forward it to [spam@uce.gov](mailto:spam@uce.gov) ([mailbump.aspx?link=mailto:spam@uce.gov](mailto:spam@uce.gov)). If you believe you've been scammed, file your complaint at [www.ftc.gov](http://www.ftc.gov) ([speedbump.aspx?link=http://www.ftc.gov](http://www.ftc.gov)). Visit <http://www.ftc.gov/spam> ([speedbump.aspx?link=http://www.ftc.gov/spam](http://www.ftc.gov/spam)) to learn other ways to avoid email scams and deal with deceptive spam.

## Protect yourself against wire fraud

Technology and the Internet have transformed and revolutionized the way that banks and consumers do business. Transactions that formerly took days to complete can now be performed in seconds. However, with the added convenience of being able to move money around the world with the click of a mouse, fraud – and more specifically, wire fraud – continues to be a lucrative business opportunity for malicious actors. Using email forgery or other impersonation techniques, they trick employees and businesses into sending money to unauthorized recipients, resulting in billions of dollars in losses over the past decade. In some cases, law enforcement has been able to reclaim the funds after they were transferred, but in others, the money is gone for good. How can you protect yourself and your company so that you don't fall victim to these scams? First, let's take a look at how it works.

### How does wire fraud work?

More often than not, thieves will use email forgery as a main method to initiate wire fraud. It is very easy today for hackers to spoof email to make it look as if it is originating from trusted companies that you may do business with. These email forgery attacks can take the form of a Business Email Compromise (BEC) where the email account of a senior executive is hacked and the malicious actor then uses this compromised account to email unsuspecting employees into performing a wire transfer on their request. Or, a lookalike domain is created by a malicious actor with a name similar to a trusted one, and the attacker then sends a wire request to a company using this new domain. The subtle change or intentional misspelling in the name could go unnoticed by the victim company, and before they realize their mistake, it's too late. Once the wire transfer has completed, the money is likely gone for good. Fortunately, there are steps that companies can take to prevent this from happening.

### Preventing wire fraud

Here are some best practices that you can take to avoid being a victim of wire fraud.

- Confirm all wire transfer requests verbally or in person. Never authorize a wire transfer through email.
- Train employees to be aware of common phishing techniques. Perform regular security awareness training.
- Be cautious of a third party requesting changes to their account number or routing number. Confirm these changes verbally with a known contact at the company.
- Be suspicious of wire transfer requests to foreign banks.

### What to do if you are a victim of wire fraud

If you believe you are a victim of wire fraud, please report it to your local branch or contact Treasury Management Service at 888-889-8369 immediately. You can also report it to your local FBI office so that they can help retrieve any transferred funds before it's too late. Always remain vigilant and train employees to be on the lookout for scams. Remember, the best defense against fraud is a good offense.

## Contact Us with Questions

For more information, please [contact us \(Contact-Us\)](#).

Copyright © 2025 CTBC Bank Corp. (USA). All Rights Reserved.

