

how to recognize and avoid phishing scams



partners bank of california

pbofca.com

Member
FDIC

how to recognize and avoid phishing scams

how to recognize phishing

Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message.



Phishing emails and text messages may look like they're from a company you know or trust.



They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.



Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment.



They may say you must confirm some personal information, want you to click on a link to make a payment, or say you're eligible to register for a government refund, to name a few.

how to recognize and avoid phishing scams

how to protect yourself from phishing attacks

Your email spam filters may keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so it's a good idea to add extra layers of protection.



Protect your computer by using security software. Set the software to update automatically so it can deal with any new security threats.



Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats.



Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication.

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.



Protect your data by backing it up. Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

what to do if you suspect a phishing attack

If you get an email or a text message that asks you to click on a link or open an attachment, answer this question: **Do I have an account with the company or know the person that contacted me?**



If the answer is “No,” it could be a phishing scam. Go back and review the tips in [How to recognize phishing](#) and look for signs of a phishing scam. If you see them, [report the message](#) and then delete it.



If the answer is “Yes,” contact the company using a phone number or website you know is real, not the information in the email. Attachments and links can install harmful malware.

how to recognize and avoid phishing scams

what to do if you respond to a phishing email

If you respond to a phishing email, there are steps you can take depending on the nature of the email.



If you think a scammer has your information, like your Social Security, credit card, or bank account number, go to [IdentityTheft.gov](https://www.identitytheft.gov). There you'll see the specific steps to take based on the information that you lost.



If you think you clicked on a link or opened an attachment that downloaded harmful software, update your computer's security software. Then run a scan.

how to recognize and avoid phishing scams

how to report phishing

If you got a phishing email or text message, report it. The information you give can help fight the scammers.



If you got a phishing email, forward it to the Anti-Phishing Working Group at reportphishing@apwg.org. If you got a phishing text message, forward it to SPAM (7726).



Report the phishing attack to the FTC at ftc.gov/complaint.