KeyBank

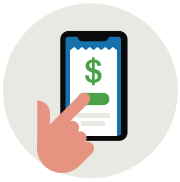
protect yourself from fraud

At KeyBank, the security of your accounts is a top priority. We're always looking for new technologies and ways to help you keep your accounts safe and secure.

Arming yourself with the latest information is crucial to protecting your financial accounts and your personal data — and we're committed to keeping you apprised of the latest fraud trends and preventative measures.

Here are a few guidelines to help you safeguard your accounts against fraud.

Use online banking and account alerts to catch suspicious activity quickly. You don't have to wait for your monthly statement to check your account activity — in fact, we recommend reviewing your transactions daily. Online banking allows you 24/7 access to your accounts so you can do just that. And once you're enrolled, you can make things even easier by setting up account alerts[1] for automated, around-the-clock monitoring of your accounts. To do so, simply sign in to online banking, scroll down to the ***I want to…*** section, then choose ***Manage Alerts***.



Check payments are most secured when mailed directly from inside your post office. With mail and check theft on the rise, you may also want to consider using other forms of payment, such as debit or credit card, or electronic methods such as online Bill Pay or Zelle.®[2]

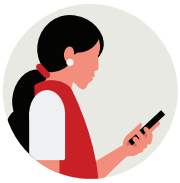
When in doubt, don't click! Embedded links are often a fraudster's bread and butter. Whether in a text message or email, you should never click on a link unless you are 100% certain it is legitimate. Other fraud techniques commonly employ embedded links to collect your sensitive data or install harmful malware on your computer. Be skeptical of any text or email containing a link. Look for red flags like a request to verify or unlock your account, a sense of urgency, or grammatical/spelling errors. If you're even the slightest bit suspicious, ***do not*** click the link.

Fraudsters often impersonate banks and can be very creative in trying to get access to your accounts. If KeyBank ever initiates a call or text to you, we will not ask for your log-in credentials, passwords, PIN, or one-time passcode. We'll also never ask you to send money to yourself via any electronic method such as *Zelle*, account transfers, or wire payments.

If you notice anything remotely suspicious, play it safe and verify the situation. If you receive a call, text, or email claiming to be from KeyBank that you feel is questionable, hang up the phone and/or do not respond to the message. **Immediately contact KeyBank through a known channel** by contacting your banker, calling or visiting your local branch, or contacting us through a phone number like 1-800-KEY2YOU.® There's no harm in verifying the legitimacy of a request — in fact, we'll be glad you did.

[1] Message and data rates may apply from your wireless carrier.
[2] Subject to terms and conditions in Service Agreement.

Protect yourself from fraud



Stay informed. When it comes to fraud, knowledge is power. Staying up to date on the latest trends and emerging scams is your greatest defense. And KeyBank is here to help you do just that. We'll continue to share information, guidelines, and best practices that will help you identify and potentially avoid fraud attempts. For additional information on trending fraud tactics and how to avoid them, visit banksneveraskthat.com.

We're here to help.

If you think you may be a victim of fraud, report the matter to KeyBank **immediately** through a known channel or by calling the KeyBank Fraud Hotline at 1-800-433-0124.

KeyBank