Key Private Bank

Fighting fraud:

The latest scams and how to protect yourself

Fraudsters are constantly looking for ways to gain your trust to gain access to and obtain funds from your account. Knowing what to look for can help stop identity theft and fraud while protecting your accounts. Start by getting to know the different types of scams below.

Impersonation scam

- Fraudsters call a client claiming to be from KeyBank, often using software to falsely manipulate caller ID to make it appear as though Key Private Bank is calling.
- The caller will state that they have identified fraudulent account activity in a client's account and that as a security measure, they must send a one time passcode (OTP) to a client's phone or mobile device.
- During the call, the individual will ask you to provide the security code they just sent, or ask for the answers to your online banking security questions. Fraudsters will then use this information to gain access to your online banking profile and your money (often while still on the line with you!).

While Key Private Bank does make outbound service calls, emails, and texts to our clients, when we contact you, we will never ask you to provide or verify:

- Your full Social Security number
- A numeric security code for a one-time password
- Your username
- Your password
- Your full account number
- Answers to security questions over the phone

Scammers use this information to reset your credentials and take over your account. Key Private Bank sends emails regarding any account-level changes to your account, such as username and password changes. If you receive an email from Key Private Bank or KeyBank regarding these types of changes that you did not initiate, please call us immediately.

Phishing/smishing scam

Fraudulent emails, phone calls, text messages, and websites designed to trick recipients into divulging personal financial information, such as credit card numbers, account user names, passwords, and Social Security numbers. These are designed to look like real pages (such as a Key Private Bank email).Always verify the email sender address before clicking on links within the messages.

Antivirus/technology refund scam

Clients may receive calls, emails, or pop-up notifications on their personal computer from fraudsters impersonating a virus protection software company. Fraudsters indicate a refund is due to an individual, and, when given access to personal information or online banking, funds are extracted instead of added.

Romance/sweetheart scam

The fraudster uses emotions to gain trust in order to take money from an unsuspecting person. Once the appearance of love and trust are established, the fraudster may create a sense of urgency and/or will begin asking for assistance in the form of money or fraudulent checks they will provide you to deposit and remit funds back to them.

Debt elimination scam

Fraudsters impersonating a reputable debt elimination or loan agency. They may request account information to initiate a one-time or recurring payment while not providing any measurable service.

The latest scams and how to protect yourself

How to protect yourself against fraud

At Key Private Bank, we work to keep your accounts safe and secure, whether you're accessing them online, through an ATM, on a mobile device, or in one of our branches. It is important that you are aware of this ongoing risk and learn how monitoring your accounts could help limit exposure to unauthorized activity.

Tips to protect yourself against fraud

- If you receive a phone call requesting any of the information above, hang up and call us immediately at 1-877-634-2968. For clients using a TDD/TTY device, please call 1-800-539-8336.
- Monitor your accounts daily. Account alerts can be set up in online and mobile banking to monitor your account balance and any debit/credit to your account and receive immediate alerts when user ID/password/personal information have been requested or changed.
- Create strong passwords that are lengthy and contain both numerals and letters. Do not use the same password for multiple sites.
- Protect your login information. Do not store it on or even beside your device.
- Create unique answers to security questions that cannot be found on the internet. Remember, only you know the answer to the question.
- Ignore spam and curb your curiosity. Phishing emails can be very subtle and may contain links or downloads infected by malware.
- Install and continually update firewall and anti-virus systems to keep unauthorized users out.

For assistance or more information on the latest scams, visit our security page at key.com/kpb/our-insights/security-and-privacy.jsp

Key Private Bank

201120-914780.02