

Citizens Bank of Northern Kentucky wants to help you protect yourself against ID theft and fraud. While internet based scams using emails, viruses and spoofed sites are popular, fraudsters may also try to contact you over the phone or through text messages. Education, awareness and knowledge of a few simple tips will make it less likely that you will fall victim to one of these scams.

REMEMBER: Citizens Bank will never ask you to send personal or financial information by email or through a link in an email.



[Safe Computing Tips \(PDF\)](#)

Download our free [Identity Theft Emergency Repair Kit \(PDF\)](#)



TIPS TO PROTECT YOURSELF

- Never provide your personal information in response to an unsolicited request.
- If you believe the contact may be legitimate, contact the financial institution yourself.
- Never provide your password over the phone or in response to an unsolicited Internet request unless you initiated the contact.
- Review account statements regularly to ensure all charges are correct.

Only our Premier Members 1st Account offers Identity WatchSM which helps you protect your identity! [Click here for more information!](#)



WHAT TO DO IF YOU BECOME A VICTIM

Contact us immediately about the situation.

If you have disclosed sensitive information, you should also contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file. The following is contact information for each bureau's fraud division:

- Equifax (800) 525-6285
- Experian (888) 397-3742
- TransUnion (800) 680-7289

If you suspect that you've received a fraudulent email targeting Citizens Bank customers, DO NOT RESPOND TO THE EMAIL! Contact us at 859-572-2660.

Another source of assistance:
[Federal Trade Commission ID Theft Site](#)

COMMON SCAMS DEFINED

Phishing: Fraudsters will send out bogus messages that appear to be from a company or government agency you may or may not do business with. These messages will attempt to convince you to either click on a link or call a number in order to get you to reveal information that can be used to steal your identity and/or access your accounts. Phishing messages may come through email, instant messages, and even text messages. The best thing to do if you believe a message may be legitimate is to contact the company using contact information that you know is valid such as a number from the phone book, or by typing the company's web address into the address by yourself.

Vishing: Vishing is the use of social engineering tactics over the telephone system in an attempt to gain personal information for fraudulent uses. Vishing is successful because it is hard for law enforcement to track and because the phone system is very trusted by the general public. Features like caller ID can now be forged and faked using modern tools to make the calls more believable. Customers should be very suspicious when receiving calls asking for personal information and should call the bank directly using a number they know is good if they question the validity of a request.

Spoofing: A "spoofed" site is one that appears to belong to a legitimate company. The site may even look like the legitimate company's site utilizing their colors and, perhaps, their logo. Typically a bogus email is received asking you to supply, confirm or update sensitive personal information by clicking on a link in the email. The goal of the criminal is to get you to enter the requested information so that they can steal it for their purposes.