



What is Identity Fraud

Phishing & Spoofing

One of the most common methods of identity fraud is through email. This is often referred to as "Phishing". The email sender will claim to be from a company or person that you know and trust. It's purpose is to get you to provide them with your private information, such as your user ID, password, account numbers, etc. If they are successful in getting your information, they will use it to access your accounts, your identity, and your financial information.

Sometimes the email itself will look like a page from the website of a company you know, or the email will provide you with a link that appears to connect to a website that you are familiar with. If you click on the link, it will bring you to a page that may look real, but in fact is "spoofed". This is referred to as "Spoofing", and is an attempt to persuade you to provide your personal information to them.

Hingham Savings will never ask you to send personal or financial information through an email link. If you receive a suspicious email that claims to be from Hingham Savings, contact us as soon as possible: 781.749.2200

Download our Anti-Phishing brochure to learn more about Identity Fraud, and look through the rest of this page for helpful hints on preventing and resolving Identity Fraud. You may also visit The FDIC Consumer Alert and Federal Trade Commission.