

CUSTOMER ALERT WEB FRAUD



On the Web, there are new types of criminals called “phishers”. These people may send very realistic emails pretending to be from your bank or some other organization you trust.

They are also using screens that pop up while you are on someone’s website trying to place an order. They may tell you your account is blocked until you update your files. Then they may ask you to provide sensitive account information like a PIN, social security number, accounts and card numbers or passwords.

Don’t Ever Give Out Personal Information – NEVER.

Please follow the following security tips.

Email Use:

- Be alert for fraudulent emails, even though they appear to be from a reputable source.
- Delete any email that requests your personal information immediately. Do not respond to it. Reputable businesses never request personal information in an email.
- Never send your personal information via an unsecured email.
- Do not open email attachments from unknown or unsolicited senders.
- Be careful when clicking on a link in an email. Even though it is identical to the actual company’s website, it could be fraudulent. To check, open a new browser window and manually type in the URL provided in the email. If they don’t match, delete the email with the suspicious link immediately.

Online Security:

- If you visit a website that is not what it claims to be, leave it immediately.
- Be sure to do business only with companies you know and trust.
- Watch carefully for imitation Websites designed to trick you into giving out personal information.
- Any sites that you do business with should have their Privacy and Security Statements. Read them carefully.
- Only provide sensitive personal or financial information when you have initiated it and only if the page is secure.
- Choose passwords or Personal Identification Numbers (PINs) that are difficult to guess and use a different password for each of your Internet accounts. Change these passwords often.
- Make sure the website is certified with a digital security certificate by clicking on the “closed lock” or “solid key” image located in the bottom bar of your browser window. A small frame with site security information will appear. Click the word “Subject” for Internet Explorer to verify that you are on the correct website. To verify the site certification authority, click the “Issuer” tab. For Netscape, click on “View Certificate” to view subject and issuer details.

Virus Protection:

- Keep current versions of your computer’s operating system and Internet browsers.
- Make sure you promptly disconnect from the Internet when you are not online.
- Keep your anti-virus software up-to-date to guard against new viruses. Download the anti-virus updates as soon as you are notified.
- Always back-up the files on your computer.



www.macatawabank.com

Member
FDIC

CUSTOMER ALERT WEB FRAUD