

Phishing Notice for
Woodlands Bank Customers:

What is “Phishing”?

Phishing involves the use of seemingly legitimate e-mail and/or web sites, which attempt to deceive consumers into disclosing personal, financial or other confidential information. The type of data the perpetrator attempts to get may include e-mail address, Social Security numbers, credit card numbers, passwords and personal identification numbers (PINs) among others. Access to this information could allow an attacker to access your account or steal your identity.

In most phishing attempts, the consumer will receive a fraudulent e-mail or be directed to a fraudulent website that will request that you “update” or “confirm” your financial or personal information in order to maintain your accounts. However, please be aware that perpetrators are using new and innovative phishing techniques to trick recipients into providing confidential information.

WOODLANDS BANK DOES NOT REQUEST PERSONAL OR CONFIDENTIAL INFORMATION VIA EMAIL OR OUR WEBSITE.

How can I stay safe online?

In order to protect yourself, please follow good security practices, including but not limited to:

- Ensure that your computer’s operating system and software applications are up-to-date with all security patches installed.
- Always use anti-virus software and ensure that it is kept up to date. Periodic scans should also be performed to ensure that your computer is free of malicious software (malware).
- Do not follow links within an unsolicited e-mail. Instead, use a bookmark or type the web address into your browser’s address bar.
- Do not open unexpected e-mail attachments due to the risk of malware.
- Review your account statements regularly and immediately report any discrepancies.

If you believe you have been the victim of a phishing attempt or have provided personal, financial or other confidential information, please contact Woodlands Bank immediately.