

What is Phishing?

Phishing (pronounced fishing) is the latest form of identity theft. It's when thieves act as if they are representing an organization and try to "hook" the consumer into providing personal information. They can dupe you into providing your Social Security number, bank account numbers, PIN numbers, passwords, mothers' maiden names and other personal information.

How does Phishing work?

By E-mail:

The most common form of phishing is by e-mail. For instance, you could receive an e-mail from Calvin B. Taylor Banking Company asking you to "reconfirm" your personal information. Unfortunately, this e-mail is not from us, but from a phisher pretending to be a representative of our company.

Typically, the e-mail contains a link to a Web site that looks like a near-replica of our site. You click onto the link and add your personal information, which goes right into the hands of identity thieves. It is important to not respond to these e-mails.

By Phone:

Phishers also use the phone to hunt for personal information. Some, posing as employers, call or send e-mails to people who have listed themselves on job search Web sites.

While phishing scams can be sophisticated, the following features are often indicators that something is suspicious.

Be aware of a potential scam if:

- Someone unexpectedly contacts you and asks for your personal information, such as your bank account number, a password or PIN, credit card number or Social Security number. Taylor Bank would not contact you for that information.
- The sender, who is supposedly a representative of our organization, asks you to confirm that you have a relationship with us. We already have that information on record.
- You are warned that your account will be "shut down" unless you reconfirm your financial information.

Calvin B. Taylor Banking Company is doing everything we can to counter this type of criminal activity. Your account protection is our top priority, so we have done the following to keep potential phishers from invading your privacy:

- We will ask you for answers to specific questions before releasing information about your account. For your protection, we will not release information if we cannot identify the caller.
- We ask that you choose passwords, for Internet Banking, that are difficult for others to guess. We require that your password be changed frequently.

If you receive an unsolicited e-mail or phone call that seems suspicious, and is allegedly from our organization, please do not reveal any information. In fact, please call us at (410) 641-1700 to verify that the request is legitimate. If you feel that you have been a victim of phishing, you can report the occurrence to US-CERT (United States Computer Emergency Readiness Team) by sending them an email at phishing-report@us-cert.gov or visit them at http://www.us-cert.gov/nav/report_phishing.html for more information. Contact the Federal Trade Commission's ID Theft Clearinghouse at www.consumer.gov/idtheft or call (877) 438-4338 for information on how to put a "fraud alert" on your files at the credit reporting bureaus. Also, be sure to notify your local law enforcement.