Email & Online Security Tips

Phishing is one of the most popular forms of e-mail fraud. It is a form of criminal activity that attempts to fraudulently acquire sensitive information such as passwords, account numbers, or financial information by masquerading as a trustworthy person or business in a seemingly official electronic communication. Phishing emails are often sent to large lists of people, expecting that some percentage of the recipients will actually have an account with the real organization. The term comes from "fishing," where bait is used to catch a fish.

In phishing, e-mail is the bait.

What protection do I have if I am a victim of phishing?

At Heritage Bank we will help you determine the best course of action based on the nature of the information that was compromised. Each situation is different. Please contact us at 985-892-4565 or visit your local branch as soon as possible if your information has been compromised. The sooner we know, the sooner we can work together to stop further compromises.

Can you give me an example of what a fraudulent e-mail may look like?

A fraudulent email will have a demanding tone and will urge you to act immediately. The email may threaten to close your account or request you reply with account information. The email may contain a fake website, which looks genuine because it mimics a popular company's website.

What should I do if I receive a phishing email?

Do not open it and delete it immediately from your inbox.

Is it safe to continue to use online banking?

Yes, banking online is a safe and convenient way to manage money and there is no reason why the Internet cannot be used with confidence. In fact, using online banking often is one of the best tools to monitor accounts 24/7.

Does Heritage Bank send out marketing emails?

Yes, we do use email to update our customers on new products, services and offers that may be of value to them. However, these emails will never ask you to respond with personal or account information.

How do criminals know I have an account with Heritage Bank?

They don't have specific information about you. They phish millions of email addresses in hopes that their targets will be among the email recipients. Remember they are casting a very broad net in hopes of catching unsuspecting customers.

Below are a few tips to help protect your personal and financial information.

Email Security Tips

- Never provide personal information in a response to an e-mail request, no matter who appears to have sent it. Legitimate companies don't ask for this information via email or in a pop-up message. This information includes: Account Numbers, Social Security Numbers, Mother's Maiden Name, User IDs and Passwords.
- Ask yourself if you have initiated contact with the agency or business that is contacting you. If the answer is "no", it is likely that the communication is an act to commit fraud.
- Do not click links provided in an e-mail. Copy and paste the link into your browser window.
- Do not open e-mails bearing attachments from un-trusted sources.
- Call the person or the organization listed in the FROM line before you respond or open any attached files if it looks suspicious.

Online Security Tips

- Google the company name with "fraud" or "scam" behind the company's name. For example: ABC Company + Fraud or ABC Company + Scam.
- Before making a purchase online, know who you are dealing with. Confirm online the seller's physical address and phone number in case you have questions or problems.
- Know exactly what you are buying. Read the fine print for the product closely and know exactly what the costs are for the product or service.
- Check out the return policies and delivery dates. If you return it, know who pays the shipping costs or restocking fees. Know when you will receive your order. A Federal Trade Commission (FTC) rule requires sellers to ship items as promised or within 30 days after the order if no specific date is promised.
- Read your bank and credit card statements immediately and check unauthorized charges or overcharges by merchants.
- Look for a "secure transaction" symbol like a lock symbol in the lower righthand corner of your web browser window, or https://.... in the address bar of the website. The 's" indicates "secured" and means the web site page uses encryption.