

AVOIDING PHISHING ATTACKS AND ID THEFT

Criminals are using many ways to commit identity theft or internet fraud. The methods used by these criminals can vary from a simple email sent to thousands or millions of email addresses requesting personal information, to sophisticated software (malware) loaded onto your PC without your knowledge through email attachments/links, or by clicking on a link from an infected website you visit. Criminals are moving to social networking sites (Facebook, Twitter, etc.) now as well.

You can help to avoid becoming a victim by following these steps:

1. Make sure your PC and internet browsers are updated whenever you are notified of patches. Regularly scan your PC with a current and well known antivirus software program.
2. Ensure that any website you visit is legitimate and trusted before clicking on any links.
3. Do not trust any email that urgently requests personal information of any kind. EagleBank and other reputable financial institutions/businesses/organizations do not send these types of email.
4. Never click on links in emails claiming to be from EagleBank, or a legitimate business or organization, until you have confirmed the email is authentic. Many phishing attacks download Trojan horse viruses and other malware onto your computer when a link in the email is clicked on.
5. Never enter your username and password until you are sure you are at a legitimate website. EagleBank or legitimate businesses will never ask you to verify a username, password, debit/ATM card number or PIN via email.
6. Do not call any number or use any link in a suspect email. Always verify the phone number through a reputable source before calling. All valid EagleBank contact numbers can be found on our website.
7. Suspect every impersonal email or those containing spelling or grammatical errors. Phishing attacks are mailed out to millions of people from foreign countries. For this reason, they are general in nature and often contain misspelled words and grammatical errors.
8. Phishing attacks often ask for personal financial information. Never fill out personal information of any kind through a form on the Internet that you have accessed via an email link. A request of this kind should be a big warning. EagleBank will never ask for this information via email.
9. Do not open email attachments unless you are expecting to receive one. Even if the sender is known to you, be careful of attachments that are forwarded to you with a generic or impersonal message. In particular, email attachments with ".exe" file extensions are potentially malicious.

10. Always report suspicious activity to the business or organization being spoofed. Contact the supposed sender via a number or email address you already use to confirm the legitimacy prior to opening any attachments or clicking on any links.
11. Monitor and reconcile your account(s) daily.
12. Do not send sensitive information via email. If you must, then send it as a password protected attachment.

You may call EagleBank at 301-986-1800, contact your local branch, or email us at onlinebanking@eaglebankcorp.com with any questions.

Resources:

<http://www.ftc.gov/bcp/index.shtml>

<http://www.antiphishing.org>

Windows Updates/Patches:

www.windowsupdate.microsoft.com;

MAC Updates:

www.apple.com/support

Antivirus/Malware Software:

www.norton.com

www.mcafee.com/OfficialSite

www.ZoneAlarm.com

www.TrendMicro.com

www.symantec.com