# ID Theft and Account Takeover Tips

- Make sure your PC, phone, and internet browsers are updated or patched whenever you are notified of their availability. Regularly scan your PC with a current and well known antivirus software program.
- Ensure that any website you visit is legitimate and trusted before clicking on any links. Be especially careful during times of national crisis (storm relief, victim support, etc.) or large scale events (Olympics, World Cup, etc.)
- Do not trust any email, text or call you receive that urgently requests personal information of any kind. EagleBank and other reputable financial institutions/businesses/organizations do not communicate in this way.
- Never click on links in emails or texts claiming to be from EagleBank, or a legitimate business or organization, until you have confirmed they are authentic. Many phishing attacks download viruses or other malware when a link is clicked on. Links may also take you to a website asking for personal information.
- 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.
- Do not call any number or use any link in a suspect email or text. Always verify the phone number through a reputable source before calling. All valid EagleBank contact numbers can be found on our website (eaglebankcorp.com).
- Never fill out personal information of any kind through a form on a site that you have accessed via an email or text link. A request of this kind should be a big warning. EagleBank will never ask for this information via email or text.
- 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. 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.
- Share as little personally identifiable information about yourself on social media sites as you can. Restrict access to these sites where possible to only persons known to you.
- Never conduct wire or ACH transactions or update vendor payment information based on email requests alone regardless of if the request comes from a boss, company executive, or known vendor contact. Always verify the request with the sender through a channel other than email.
- Monitor and reconcile your account(s) daily and set up online banking alerts.
- Do not use the same password for multiple sites or easy to guess passwords. Consider changing passwords on a scheduled basis.
- Whenever an option, turn on two-factor authentication for any online account updates that allow you to change a password or contact information.
- Request a copy of your credit report at least annually.

# ID Theft and Account Takeover Tips

**Additional steps to help protect you on your phone:**

- Do not attempt to alter the default functionality of the operating system outside of the standard security setting options. Commonly referred to as “jail breaking” or “rooting”.
- Never install apps from any place other than iTunes for Apple devices and the Google Play Store for Android and do not adjust any security setting to bypass this default restriction.
- Carefully review permissions an app is asking for prior to allowing them.
- Have your phone lock after a period of inactivity. If not using biometrics, make sure you use a secure password.
- Never connect to an unsecured wifi network (password free ones at coffee shops, airports, stores, etc).
- Do not store any non-public data (passwords, account numbers, medications, etc) in unsecured or unencrypted apps.

You may call EagleBank at 301-628-4708, contact your local branch, or email us at customercarecenter@eaglebankcorp.com with any questions.

Resources:
http://www.ftc.gov/bcp/index.shtml
http://staysafeonline.org
http://www.ic3.gov

Credit Report Information:
http://www.annualcreditreport.com/

Windows Updates/Patches:
www.microsoft.com

MAC Updates:
www.apple.com/support