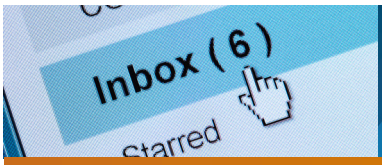

Access National Bank
The Difference is Access.

TIPS ON WHAT TO DO IF YOUR EMAIL IS HACKED

1. **Change Your Password**
   - Use 10-12 characters or more in your password, the longer the better. Mix upper and lower case letters, use symbols and numbers. Don't recycle an old password.
   - Don't use birthdays, addresses, kids' names, dogs' names, maiden names, favorite movie names, favorite band names, or anything else that you might otherwise feature on your Facebook page or that is public knowledge.
   - If you used the same password for other accounts like social media or online banking, change those passwords too.

2. **Report the Incident to your Email Provider**
   - Your email provider has seen this type of thing before and may be able to provide you with further details about the nature and source of the attack, as well as any tools they may have available to protect your information and get you back up and running.
   - Sign up for two-factor authentication, if you have Gmail, Microsoft's Outlook.com and Hotmail and Yahoo!.

3. **Alert Your Contacts**
   - Notify everyone on your contact list that you have been compromised and they should look at any communication from you with suspicion for the time being. Further, they should check their computer protection. The sooner that you let them know that the account was hacked, they'll know any such request from you may be bogus and not to respond or click on links within the email.

4. **Scan your Computer with Updated Anti-virus and Anti-malware Programs**

5. **Review your Personal Email Settings**
   - Make sure the cyber criminals haven't created forwarding email addresses and if you find any delete them immediately.

6. **Check Related Accounts**
   - While the hacker has access to your account, they have access to your entire email box including both what is in your account now, past email, and any incoming email.

7. **Change Passwords or Security Questions for Other Sites.**

8. **Check your Email Folders.**
   - People have a tendency to send financial or personally identifiable information to others via email and then archive the email in a file in their system. If so, immediately go to whatever account is identified and change the user ID and password.

9. **Monitor your Personal Information.**
   - Assuming that the hacker in question was able to find valuable pieces of personally identifiable information, it will become important for you to monitor your credit and various financial accounts for suspicious activity. You can get a free copy of your credit report, annually, at www.annualcreditreport.com. If you find any suspicious activity, you may wish to contact the fraud department of one of the three major credit reporting agencies and have a fraud alert put on your file. A fraud alert is free and the initial alert stays on your alert for 90 days.
     - **Equifax: 1-800-525-6285**
     - **Experian: 1-888-397-3742**
     - **TransUnion: 1-800-680-7289**

10. **Additional Safeguards**
    - Use long passwords that can't be guessed and don't share them with anyone.
    - Don't fall for email phishing attempts. **If they ask for your password, the email is bogus**. Don't share your password with anyone.
    - **Don't click on links in email.** Many phishing attempts lead you to bogus sites that ask you to login and then steal your information.
    - If you're using Wi-Fi hotspots, learn to use them safely.
    - Keep the operating system and other software on your machine up-to-date and run up-to-date anti-malware tools.
    - Learn to use the internet safely.
    - Consider multi-factor authentication, where simply knowing the password is not enough to gain access.