PHISHING

Internet "phishing" involves a bogus e-mail message that uses legitimate-looking materials, like another company's logo, to entice you to provide personal financial details, such as account information, credit card, and Social Security numbers. **Remember, Morton Credit Union will NOT ask you to update your information through e-mailed link or a cell phone text message. Should you receive an e-mail or text message allegedly from Morton Credit Union requesting such an update, please contact us immediately.**

How to identify them?

1. **A generic greeting is used such as "Dear Customer", instead of using your name.**
2. **The e-mails have a sense of urgency.** This may include an urgent warning requiring your immediate action.
3. **May include a warning that your account will be shut down unless you reply.**
4. The sender's e-mail address may be forged, even if it looks legitimate.
5. There is often a link to a web site to "fix" your account. These are often forged.
6. **Personal information is requested.** This may include asking for login and password information, either in the e-mail or from the link.

How to protect yourself?

1. Never respond to an unsolicited e-mail that asks for personal financial information.
2. Avoid filling out forms in e-mail messages. You don't know where the data will be sent. You should only communicate information such as credit card numbers or account information via a secured website or telephone.
3. Type web addresses into browsers instead of clicking on links in e-mails.
4. If you go to a link offered in an unsolicited e-mail, check to see if there is an 's' after the http in the address and a picture of a padlock at the bottom of the screen that indicates the link is secure and encrypts data. Though this is not an indication that the site is legitimate, an online form that asks a consumer to submit sensitive personal information should always be encrypted.
5. Closely read your e-mails before responding with any information and contact the organization if you are in doubt.
6. Be cautious about opening attachments or downloading files from e-mail messages.
7. Keep anti-virus and anti-spam filtering software on your computers, and keep it up to date.

If you've been Phished:

1. Immediately contact those organizations for which you provided the information.
2. Contact the three major credit bureaus and request that a fraud alert be placed on your credit report.

   Equifax – 800-525-6285 www.equifax.com
   Experian – 888-397-3742 www.experian.com
   Transunion – 800-680-7289 www.transunion.com

3. File a complaint with the Federal Trade Commission at www.ftc.gov or 877-382-4357.