

## Beware of Holiday Scams

Along with the holidays comes an increase in phishing scams and other online fraudsters. Northeast Credit Union, your trusted neighbor, has put together the following tips that can help protect you from online scams and fraudulent email requests:

- Review the URL carefully. Many phishers and fraudsters use a slightly different web address than the legitimate one to fool you into providing them with your personal information.
- While shopping online, look for the website address bar to include “https” and the yellow padlock in the lower part of the web page to make sure the website is secure before providing your credit card information. If the website is missing one of these components, it’s safer to call in to place the order rather than take the risk.
- Keep your Internet browser software up-to-date and use anti-virus and anti-spam software to keep your computer protected.
- Be skeptical of urgent or high-pressure messages requiring you to provide personal information such as passwords and PIN numbers. A legitimate organization would never ask you to provide this information.
- If you don’t recognize the sender of an email – delete it. Never buy anything from an unsolicited email, no matter how good of a deal it may be.
- Junk mail is just that – junk. Emails from people in other countries asking for help, claiming you won a lottery you did not enter or asking you to allow them to transfer money into your account are *all scams*.
- We live in a time where we must be suspicious of all charitable requests. It’s best to ask for information about the organization in writing and do some research about how the donation is actually used *before* determining if it’s a cause worthy of your money.