Latest Telephone Scam Attempts to Steal Debit Card Information!

Beware of a new Debit Card telephone scam that uses an automated telephone call to trick you! The scam is reported to be a recorded message stating that your Debit Card has been suspended, telling the call recipient that they must enter their debit card number. The message asks for other Debit Card information, such as expiration date and PINs. Consumers should hang up immediately.

NEVER give personal or account information to anyone who contacts you by telephone or email.

If you have received this type of call and provided debit card or other information you should notify your financial institution as soon as possible. Primary Bank customers should contact our Operations Department at (603) 310-7200 during our normal business hours.

Also,
Be wary of checks from unknown parties…

Have you ever received an offer involving a large check to be deposited into your account with instructions to wire some of that money back, perhaps to someone from another country? If you follow those instructions, you may end up owing thousands of dollars to your financial institution. Be wary of checks from unknown parties.

How to protect yourself: Ask questions, and bring the check with the instructions you received to your financial institution. Most of the time, they can help you determine the validity of the check you received.

Stay Safe Online! Increase your Internet protection by following these simple tips:

- **Always** have up-to-date anti-virus software installed on your computer.
- **Never connect** to your bank account on public computers.
- **Do not respond** to any e-mail that warns of dire consequences.
- **Remember to log-out** when you have completed an Internet banking session.
- **Create complex** passwords, **never divulge** the password to anyone, and **change** password frequently.
- **Never post personal information or your location** on social networking sites.
- **Install a firewall**, making sure your pop-up blocker is turned on in your Internet security options.
- **Be aware of anyone looking over your shoulder** when using the Internet in public places.
- **Make sure** your Wi-Fi network is password protected.
- **Choose** credit card over debit card for payment when shopping online.
- **Limit** the amount of personal info you post in social forums.
- **Apply software** updates as soon as they are released.
- **Beware of suspicious emails** containing links and attachments – even those coming from known addresses.
- When working on your PC, **use the administrative role only when making software changes.** The rest of the time, sign in as a user with limited rights.