Blue Mountain Credit Union reminds its members that they should be on high alert for unsolicited emails, advertisements, and requests for donations from potentially fraudulent charitable organizations. Malicious actors use a variety of tactics to try to compel you to engage with their efforts that can ultimately result in security breaches, identify theft and financial loss.

We share some of our best practices, tips, and suggestions below to ensure you stay safe and secure online.

- **Stay Alert** – If something looks suspicious while you are navigating the internet and shopping, *stop and think* before you click.
- **Shop Smart** – Whenever possible, do business with reputable vendors and make sure when you are using search engines you are confirming that you are being re-directed to the intended vendor's site.
- **Use Trusted Sites** – Your security is as safe and secure as your vendors. Make sure your information is encrypted, many sites use secure sockets layer (SSL) to encrypt information, this is another layer of security that will help combat potential hackers.
- **Avoid Phishing Attempts** – Phishing attacks can be complex and timely; make sure to check the email addresses that you are communicating with. It is not uncommon for an attacker to masquerade as a trusted third-party vendor attempt to secure personal or financial information. These phishing emails may even come in sandwiched between two legitimate emails from the same vendor.
- **Be Suspicious**: If a vendor is asking for information that they shouldn't have any need for (e.g. a social security or account number) it can be a clue that something isn't right.
- **Be Generous, But Wise** – We all like to give back to our community but, do so with caution. Whether you are solicited through social media, calls, texts or door to door solicitations, we recommend only contributing to organizations that you trust.

If at any time, you believe you are a victim of a scam or malware campaign, we recommend taking the following action:

- Contact Blue Mountain Credit Union at 509.526.4562
- Immediately change any passwords that may have been compromised, make sure to make a complex password using characters, symbols, and numbers.
- Report the attack to the police, and file reports with the Federal Trade Commission and the FBI's Internet Crime Complaint Center.