Phishing Scams

As we enter tax season, we want to remind everyone to remain especially vigilant against phishing attempts and other online scams. This time of year often brings a significant increase in fraudulent emails, texts, and phone calls that appear to come from the IRS, financial institutions, or trusted services requesting sensitive information.

Please remember: The IRS will *never* contact you by email, text message, or social media to request personal or financial information. Any message claiming otherwise is a scam.

Key things to watch out for during tax season:

1. **Emails or messages claiming to be from the IRS or tax services**
   Scammers often impersonate the IRS to request W-2s, Social Security numbers, tax forms, or login credentials.
    a. Do **not** click links.
    b. Do **not** download attachments.
    c. Do **not** reply with any personal information.
2. **Requests for confidential or financial information:**
   No legitimate organization — internal or external — will ever ask you to send passwords, tax documents, banking details, or personal data over email.
3. **"Urgent" or "Account locked" messages:**
   Fraudulent messages often use threats or urgency to push users into acting quickly. Always take a moment to verify the source.
4. **More sophisticated phishing due to AI:**
   Generative AI makes it easier for attackers to produce highly convincing emails that:
    a. Use correct grammar and professional tone.
    b. Reference your department or role.
    c. Mimic internal communication styles.
    d. Personalize details gathered from public information.

Please be aware that even experienced users can be fooled by these new, more tailored phishing attempts.

How to protect yourself and the organization:

a. **Verify the sender:** Check the email domain carefully. Small variations may indicate fraud.

b. **Hover before you click:** Inspect links before opening them.

c. **Report suspicious messages immediately:** Use the *Report Phishing* button in Outlook or forward the email to the IT department.

d. **Email** the IT Security team using itsecurity@bamsi.org.

e. **When in doubt, don't interact:** It's always safer to double-check with IT before responding or clicking anything questionable.

Always feel free to reach out to IT if you have any questions or concerns.