**Don’t Take the Bait**

“Update your account now.” “You just won a cruise!” “The IRS has a refund waiting for you.” A group of business folks with which I was meeting last week had experienced these lines. It is time for a quick reminder about cyber practice and security.

In the cyber world of phishing, these sentences are “bait” – lures from emails, telephone calls and texts all designed to separate you from your cash, your passwords, your social security number or your very identity.

It is extremely important that small business CEOs protect their personal and company’s data. Remind your people often about the lure of these phishing tactics.

The IRS has teamed up with state revenue departments and the tax industry to make sure you understand the dangers to your personal and company’s financial data.

No doubt you’ve heard that warning to beware of phishing many times. But, phishing remains a problem because it works. Cybercriminals on a daily basis concoct new ways to trick people into turning over cash or sensitive data that can affect your taxes.

When it comes to this type of crime, the main line of defense is not technology, it is you and your people.

Criminals pose as a person or organization you trust and/or recognize. They may hack a friend’s email account and send mass emails under their name. They may pose as your bank, credit card company or tax software provider. Or, they may pose as a state, local or federal agency such as the Internal Revenue Service or a state agency. Criminals go to great lengths to create websites that appear legitimate but contain phony log-in pages.

Just remember: No legitimate organization – not your bank, not your tax software company, not the IRS – will ever ask for sensitive information through unsecured methods such as emails. And the IRS never sends unsolicited emails or makes calls with threats of lawsuits or jail.

Scam emails and websites also can infect your computer with malware without you even knowing it. The malware can give the criminal access to your device, enabling them to access all your sensitive files or track your keyboard strokes, exposing login information.
Here are a few simple steps you can take to protect yourself:

✓ Avoid suspicious phishing emails that appear to be from the IRS or other companies; do not click on the links- go directly to their websites instead.
✓ Beware of phishing scams asking you to update or verify your accounts.
✓ To avoid malware, don’t open attachments in emails unless you know who sent it and what it contains.
✓ Download and install software only from websites you know and trust.
✓ Use security software to block pop-up ads, which can contain viruses.
✓ Ensure your family understands safe online and computer habits.

To learn additional steps you can take to protect your personal and financial data, I have found a very informative article on the IRS website. You can find it at https://www.irs.gov/Individuals/Taxes-Security-Together

Each and every taxpayer has a set of fundamental rights they should be aware of when dealing with the IRS. These are your “Taxpayer Bill of Rights”. Explore your rights and our obligations to protect them on IRS.gov.

______________________________
Dean L. Swanson
Southeast Minnesota SCORE
c/o Rochester Area Chamber of Commerce
220 South Broadway, Suite 100
Rochester, MN 55904
www.seminnesota.score.org/
*Dean is a volunteer SCORE Mentor and Regional Vice President for the North West Region