Scammers posing as IRS use credible emails to threaten victims

Scammers, impersonating the Internal Revenue Service, are perfecting the art of fraud by targeting users of Microsoft's Office 365.

The fake email claims it has been sent to collect payments and also threatens to press legal charges.

It appears to originate from the "irs.gov" domain that is a credible *impersonation* of the IRS.

Both the spoofed 'irs.gov' sender domain and the specific ID's assigned to the recipient, give the email a false sense of legitimacy. Additionally, the email creates a sense of authority through its tone and professional language.

That, combined with urgency, a key component of most legal scams, can cause victims to act rashly and pay off outstanding debts in order to avoid arrest. The fraudster also claims that they have contacted the person before and that the case has escalated. This is meant to provoke immediate action, as the recipient may feel they cannot delay their payment any longer.

The email also contains specific language such as unique account and loan numbers, as well as docket and warrant IDs. By using seemingly specific information, the attacker strengthens the aura of legitimacy of the attack, increasing the likelihood of the victim engaging.

According to an advisory from the IRS, the IRS will <u>NEVER</u> initiate contact with taxpayers via email about a tax bill, refund, or Economic Impact Payments.

Additionally, the IRS cautions those who may receive these nefarious e-mails, **NOT** to click on links claiming to be from the IRS, and to be very wary of emails and websites − they may be nothing more than scams to steal personal information.

Submitted by Barb Kanehl, Chair, Neighborhood Watch
(Information gleaned from article on Fox Business News 11/12/20)