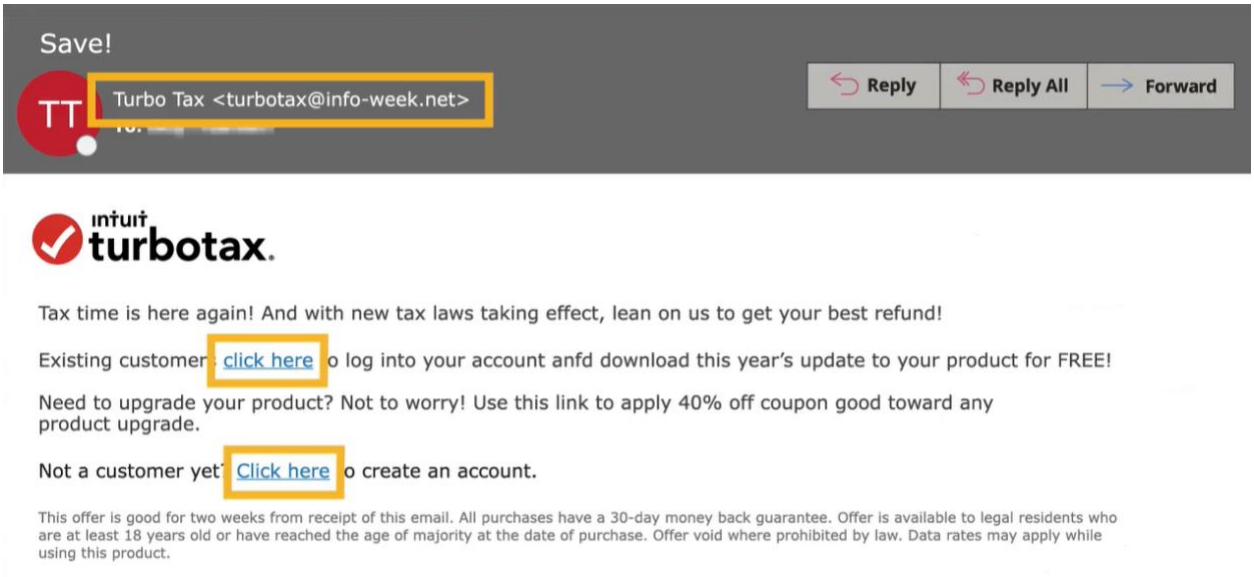
This Month's Tip: Tax-Related Phishing

Tax season is upon us, along with a perennial threat: tax-related phishing attacks.
These attacks are particularly dangerous because they tend to target sensitive information and they can give cybercriminals direct access to an individual's or an organization's money. Tax-related phishing emails often impersonate government tax agencies or organizations that assist with tax preparation and filing.

Here is an example:



First, look at the sender details. Does the sender address fully match what you would expect? This email was sent from **info-week.net** instead of the company's official domain.

Second, note any language that urges you to click a link or download an attachment. While many phishing attacks try to trigger fear or concern, this message offers an enticing discount. Threat actors hope this offer will prompt the recipient to ask fast without thinking.

Tax-related phishing could affect both business and personal accounts, so it's important to stay alert. If you receive a questionable or suspicious email at work, immediately report it. Here are several tips to keep you safe this tax season:

• Know the email polices of your tax agency and tax preparer. Most will not initiate contact via email to request sensitive information or ask that you to download something.

• Don't click links or call phone numbers in unsolicited emails. Always use a trusted contact, like an online bookmark or a phone number you have used before.

• Act quickly if you suspect fallen for a tax-related phish. Contact the appropriate organizations and change any affected logins.

• Always report suspicious emails to the Supreme Lending Cyber Security Team via the Outlook "Report Phish" button.

If you have any questions regarding this tip, please contact Information Security via Mark.Nagiel@SupremeLending.com. Thanks for participating in the information security effort!