Written by Drew Zimmerman, Daily Vidette Senior Staff
Thursday, 23 February 2012 13:44

The Central Illinois Better Business Bureau is alerting taxpayers about the potential threat of a phishing scam that aims to target one's financial information.

The email, which claims to be from the IRS and has a subject line that reads "Tax Refund Notification," stated consumers are able to receive a $655 refund. Taxpayers are then directed to a third party website where phishers can access personal and financial information.

The IRS and the Justice Department are working together to shut down these illegal operations, according to Jessica Tharp, vice president of Central Illinois BBB.

"Taxpayers who knowingly or unwittingly get involved must repay all taxes due plus interest and penalties," Tharp said.

Other phishing scams involve tax preparation. IRS investigators say that preparers may use personal information to file falsified returns and keep most of the fraudulent refund. It is important to note the taxpayer is ultimately responsible for the accuracy of all information on a tax return, even if someone else prepares it, Tharp added.

Preparers may also offer anticipation loans that allow taxpayers to leave with a check or debit card instead of waiting for the IRS to mail the refund. The BBB advises consumers to avoid these loans, which can carry interest rates from 50 to 500 percent, and may also contain hidden administrative fees.

"If a preparer makes a mistake in calculating your refund, borrowers may have to pay fines and fees. In most cases, tax refund anticipation loans only give consumers their refund a few days faster than the IRS, which can direct deposit your refund in as few as 10 days," Tharp said.

Before meeting with a preparer, Tharp advises taxpayers to ask for referrals from friends, check credentials, be wary of promises, read the contract, and check their return.

In addition to email scams, phishing via text messages has also emerged this past year.

Text phishing is relatively new and tougher to contain, but the tips banks provide to consumers to prevent these scams are generally the same, according to Linda Koch, president of the Illinois Banking Association.

“It’s tougher because not every bank knows their customers cell phone numbers, but it’s important not to give information to unsolicited emails and texts, and always check your credit card statements,” Koch said.

Most banks also use software that detects unusual spending from a consumer’s account, she added. According to Koch, 29 to 30 percent of the nationwide banking industry has reported phishing losses.

Information on how to avoid phishing scams and identity theft is available on the ISU University Computer Help Desk website. It’s important for a student to use their ULID and university email strictly for academic purposes.

The Help Desk advises students use five strategies to avoid phishing scams, which include being skeptical, verifying the web and email address, look for signs of security, look for “phishy” details, and make a phone call to the company to verify.