Consumer Alert – Beware of Scammers

TSB cautions consumers to beware of scammers pretending to be from Microsoft, Telstra or another major software company. Scammers target victims by both email and/or phone calls claiming to be from Microsoft. The gist of the message is that they have detected a problem with your software or will offer to assist you with a recent upgrade.

Here is how it works:

- You receive an email of phone call claiming that they can assist with an upgrade, or that a problem has been detected
- You will be directed to click on a link or visit a website to download software. The website, while it may look legitimate, is not.
- The software is ransomware, which will lock you out and demand payment. If you pay, your money will be gone.
- They may request remote access to your computer to assist with the error messages. Once in, they can wreak havoc on your computer, copy data files, and steal passwords.

Warning Signs:

- You receive a phone call out of the blue by someone claiming to offer tech support.
- They tell you they need remote access to fix the problem.
- They try to get you to buy software.
- They ask for personal information, such as your bank account number and/or social security number.
- Caller is extremely persistent.

If you receive a call or email claiming technical support with a request to remote in or sell you software, hang up or delete the email. Never provide remote access to your computer to anyone that you don't know and don't click on unknown links or files. If you think you have fallen victim to a scam, contact your local police department immediately.