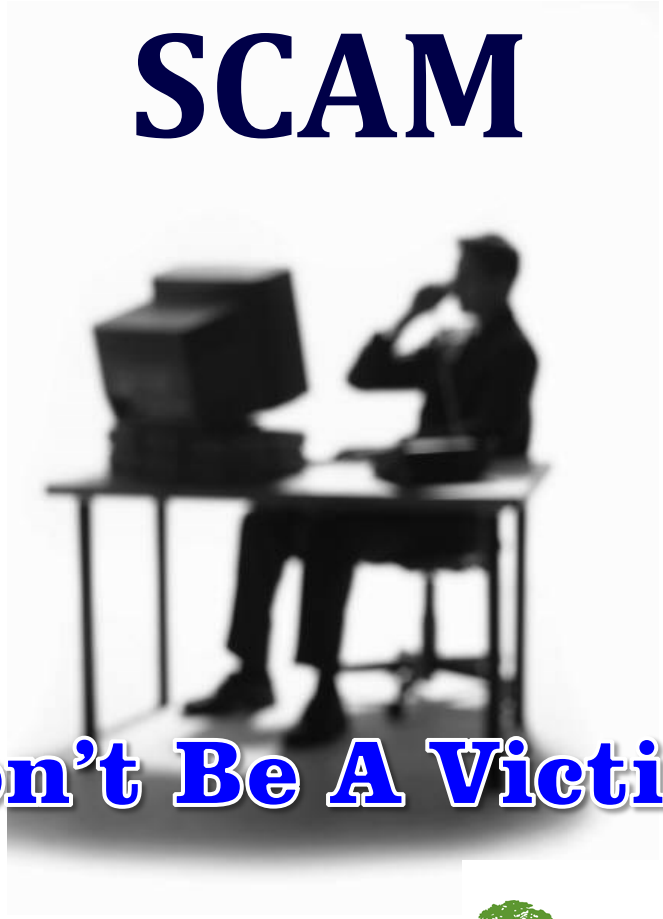
ALERT BULLETIN

COMPUTER SCAM



Don't Be A Victim!

Lisle™
THE ARBORETUM VILLAGE

COMPUTER SCAM

TYPE OF SCAM

Telephone call from Microsoft or Apple Technical Support (male or female) usually with a distinct foreign accent. They may also say they are from Windows Technical Support.

DESCRIPTION OF THE SCAM

The call can originate from any area code in the country. If you have caller ID, you may see that it is shown as a cellphone call, but not always.

The caller identifies himself/ herself as Technical Support team from Microsoft, Windows or Apple. Here is an example: *"Sir/ Madam! your PC operating system License is either illegal or has expired. You have to renew the license immediately or your PC will not work properly and will be likely to receive a vicious virus attack".* The caller would inform you that he/she will show you how to find this information for your PC. This usually involves the caller asking you to close all windows and open a specific webpage (one reported web site is "www.amyy.com"). That webpage will identify your PC/Mac/iPad as having an expired license.

Another variant of this scam involves the supposed Technical Support team representative from Microsoft, Windows or Apple telling you that they have detected that you have a problem with Windows, Mac OS, iPad iOS, etc. They will offer to fix the problem for you by directing you to a website where the "fix" will be downloaded to your computer.

In both cases, virus software will be downloaded onto your com-

puter. After this happens, you will find that you cannot use your computer any longer. Or, that your computer begins to malfunction. This type of virus is known as "ransom-ware". You may also find that the scammer now has all of your passwords and account numbers.

What the Scammer Want$

MONEY! The scammer wants you to send them money to unlock your computer. Usually they want you to send a wire transfer or some type of money-gram. They may demand this during the initial phone call or they may call back later, after you have had time to experience the ransom-ware that they just put on your computer. The scammer knows that the vast majority of home computer users have no idea how to get this ransom-ware off their PC. If you do a wire transfer the scammer now has a way to get additional funds from your bank account.

Your Response

HANG-UP! ***DO NOT*** follow their instructions! And ***NEVER*** pay them any money and ***NEVER*** give them any personal information. If you do not follow these tips, the scammer will ***LOCK YOUR COMPUTER*** until you pay the ransom.

Please keep in mind … Microsoft and Apple technical support will not call you, unless you call them first. Plus, there is no way for Microsoft and Apple to know if your Windows or Apple product; such as, a Mac, iPad or iPhone has problems or not.

Victim of this Scam

The Federal Trade Commission (FTC), Microsoft and Apple are aware of these scams. If you become a victim of this scam Go to this official FTC website to file a complaint: *http://www.consumer.ftc.gov/articles/0076-phone-scams* and click on "file a complaint with the FTC."

Microsoft:

https://support.microsoft.com/contactus/emailcontact.aspx?scid=sw;en;1671&ws=reportabuse

Apple Support Center: 1-800-275-2273.

Further Information

Here are some links which explain this scam in full detail.

- http://www.consumer.ftc.gov/articles/0076-phone-scams
- http://www.microsoft.com/security/online-privacy/msname.aspx
- http://www.forbes.com/sites/marcochiappetta/2014/08/25/scamming-fake-microsoft-support-scammers

For Additional Information or Report an Incident Contact

Lisle Police Department at 630-271-4200 or 911

This bulletin was prepared by the Volunteers In Police Services Unit of the Lisle Police Department