June 2013

Fraud Alert!

C.A.S.E.
Churches Against Senior Exploitation

Weld County District Attorney Kenneth R. Buck
Assistant District Attorney Michael J. Rourke

Don't fall into the "tech support" trap!

A recent upsurge has been reported in scammers trying to gain access to bank accounts, credit cards and other information by posing as technical support for your computer.

They use personal information and technical jargon to convince people they are legitimate and trying to protect the resident's computer from unauthorized access, when in fact, they are trying to get into digital files to steal and make money. Don't fall into this trap.

The con artist will call and pretend to be from a computer or software company and claim that the resident's computer has been compromised and needs protection. From there, the caller could try several different ways to steal from the person they are claiming to help:

- They could try to sell fake protection software. This could be protection available for free elsewhere on the internet or could actually be malware that will leave a person's computer vulnerable.
- They could ask for a credit card payment to protect the computer or could route the caller to an unsecure page to pay the fee – a page where they will be able to access the credit card and other personal information to lead to identity theft.
- They could ask for a computer password and the authority to fix the computer remotely, instead giving the scammer free rein into all bank accounts and personal information stored on the computer.

If you receive a call like this, the best thing to do is hang up and call authorities. Software and computer companies will not call someone and ask for passwords or request permission to do a security scan. Microsoft, one of the largest software companies, even warns against this scam on its web site.

Prevent Fraud

- ☑ Never allow a solicitor remote access to your computer.
- ☑ Never reveal personal or financial information over the phone.
- ☑ Always verify a business/caller is legitimate before doing business with them. For tech support claims, hang up and call the number printed on your original software paperwork.

Under no circumstances should you give out your passwords, credit card information or access to your computer.

But if you do, immediately change all your passwords and install legitimate security software on your computer and have it scan for problems or issues. Also, flag your credit cards for potential fraud.

If you do not give out your information but are still worried about the security of your computer, you can call the company itself.

But do not rely on phone numbers found online or even on caller ID as these can be manipulated. Instead, look on the official software package for a phone number.

Immediately report to your local police agency if you think you are a victim of crime.
To view other Fraud Alerts, go to www.weldda.com.