Year 2020 Date Scam

The new calendar year has given scammers a new opportunity, the potential to forge 2020 documents. To prevent this DO NOT abbreviate the year on any of your paperwork. The abbreviation can easily be changed and used against you. As an example, scammers can simply manipulate a document dated 2/15/20 to read 2/15/2000 or even 2/15/2021. Writing out the full date can help you protect yourself against legal issues on paperwork.

This scam could possibly be used to create an unpaid dept or even an attempt to cash an old check. For example, paperwork may state that the payments start on 1/15/20, the scammer could possibly edit the document changing the date of your obligation to pay back to 1/15/2019 and then try to collect the additional back "unpaid" amount. In the future, a check dated with the abbreviated date of '20 could become 2021 next year which could possibly make this uncashed check active again.

Windows 7 Scam

Microsoft has announced that they are no longer providing technical assistance, software updates or bug fixes for Windows 7. This announcement has given scammers an opportunity to extort money from those still using this operating system.

You receive a call from someone who claims to be a concerned Microsoft employee. They explain that you need to upgrade your operating system if you want your computer to keep working. The caller may say that you need to upgrade from Windows 7 to Windows 10, or simply that your Windows license is expiring. They may convince you to pay yearly fees, that actually do not exist, or request remote access to your computer under the guise of installing software. If you pay the fees, you could lose hundreds of dollars. If you allow the scammer remote access to your computer, your secure personal information, such as banking details and login credentials, can be compromised. This puts you at risk for identity theft.

Microsoft has confirmed through the Better Business Bureau that they do not reach out to offer support by phone or pop-ups on your computer screen. All support requests are initiated by the customer.

There are a few ways to protect yourself from Tech Scams:

1. Do not trust unsolicited callers (companies that do not call consumers without their permission).
2. Double check any unusual claims, do not take a caller's word for an issue you had no idea existed. Research first!
3. Never allow a stranger to remote access your computer.
4. Get your technical information straight from the source (call the company direct using the support line).

If you have concerns regarding scams or fraudulent activity, please do not hesitate to call the Department for information or assistance. If you have any question on the validity of calls, mail or email that you may receive we are happy to investigate to the best of our ability the legitimacy of these instances. And as always, please do not hesitate to call me at 413-628-4441 extension 1 or stop in at the Department, my door is always open.