HAVERFORD TOWNSHIP POLICE DEPARTMENT

1010 Darby Road Havertown, Pennsylvania 19083

Community Notice

Scam Alert – Microsoft Security Experts

HTPD has received numerous complaints about a popular phone scam that has been occurring.
Please be advised that should you receive a phone call from a security 'expert' offering to fix your PC - it's a scam. Here are some suggestions to avoid the 'Microsoft phone scam', and what to do if you fear you have fallen victim to it. This 'Microsoft phone scam' first became popular in mid 2009, and peaked in September 2011. But the scam is still around, and recent experiences suggest lots of people are being caught off guard. So here is how to avoid the 'Microsoft phone scam' in the first place, and what to do if you are a victim

Microsoft phone scam: how it works

A scammer calls you, and asks for you by name. They say they are a computer security expert from Microsoft (or another legitimate tech company). The 'security expert' is plausible and polite, but officious. They say that your personal computer or laptop has been infected with malware, and that they can help you solve the problem. What happens now depends on the particular strain of scam with which you have been targeted. Some crooks will ask you to give them remote access to your PC or laptop, and then use the access to harness your personal data. Others get you to download malware that will do that task for you. A more straightforward scam is to simply ask for money in return for a lifetime of 'protection' from the malware they pretend is on your machine. Here's the important bit: **no legitimate IT security pro is ever going to call you in this way.**

For one thing, they can't tell that your PC is infected. They've got your name from the phone book, or any one of the thousands of marketing lists on which your details probably reside. They know nothing about your home computing set up - it's a fishing trip to see if they can hook some low-hanging fruit (forgive the torturous mixed metaphors). Basically, somebody is sitting in a room calling number after number hoping to find a victim. It's not personal, but it is ultimately dangerous to your financial and technological health.

Microsoft phone scam: what to do if you are called:

1. **END** the call immediately. It is not a legitimate call.
2. **NEVER** provide any personal information. This is a good rule for any unsolicited call. Certainly never hand over your credit card or bank details.
3. If you've got this far, we can only reiterate point number 1: **END the call**. But whatever you do don't allow a stranger to guide you to a certain webpage, or instruct you to change a setting on your PC or download software.
4. If possible get the caller's details. Ask for a call back number. Write it down but do not call them back. You should report any instance of this scam to the police.

5. Finally, change any passwords and usernames that could plausibly have been compromised, and run a scan with up-to-date security software. Then ensure that your firewall and antivirus are up to date and protecting your PC.

Microsoft phone scam: what to do if you have been a victim:

Do not beat yourself up. This could happen to anyone (and does). First of all, you need to change all the personal data that you can change. As much as you might like to you can't change your date of birth, and changing your name and address seems extreme. But you can change all your passwords and usernames, starting with your main email account and any bank and credit card logins. Also, contact your bank to ask them to be on the lookout for anything unusual. Use up-to-date security software to scan and cleanse your PC, and if the scammer did get you to do something to your PC using System Restore to roll back the settings is always a good idea. Contact the police. If you have lost money, it's possible your Credit Card Company or insurance will cover the loss.

Finally, if you feel you may have been a victim of any phone scam please contact Haverford Township Police Department by calling 911.