# Avoid Phone Scams (Vishing)

Stephanie Obodda - 2016-01-25 - 0 Comments - in Phishing

In addition to phishing emails, scams can originate via the telephone (sometimes called "vishing" for voice phishing). The most common scams are Microsoft support and printer-related. Another reported phone scam asks for your email address to send you information, often to send you information that you will then be charged for. *Example: phone number 208-231-1644 as documented in these entries from 800notes.com.*

***Microsoft Support Scam:***

A common scenario is an intended victim getting a phone call, often from someone with a heavy accent, who claims to be from "Microsoft tech support." The person is calling to alert the victim that their computer has been hacked and offers assistance to recover the computer. When pressed for details, the caller is vague, will repeat sentences from a prepared script, and if pushed hard enough will just hang up. For those with caller ID, the call usually appears as an "unknown number."

Microsoft is aware of this scam and posted this article with background and safety tips about them: www.microsoft.com/security/online-privacy/avoid-phone-scams.aspx. They recently added this article: blogs.microsoft.com/cybertrust/2014/09/18/how-to-report-the-microsoft-phone-scam/. Mac users are not immune as they may be called as well (last year there was an article about targeted Mac users).

ISG reminds you that Microsoft would not call you directly.

*More information:*
http://www.consumer.ftc.gov/blog/ftc-combats-tech-support-scams
http://www.consumer.ftc.gov/blog/tech-support-scams-part-2
http://www.consumer.ftc.gov/articles/0076-phone-scams

***HP Printer Scam:***

A typical scam begins with a phone call from someone identifying themselves as being an individual on campus requesting printer model numbers or offering toner for printers or copiers. The caller usually is checking for some level of trust (will the person provide the model number), looking for victims. For some who fall for this, toner is then shipped to the individual who is charged at prices up to three times the typical amount. The caller may

also be seeking a printer's IP address, which could provide the scammer with remote access to the printer.

ISG suggests that you use caution when giving information over the phone, especially in situations when the supposed vendor makes the contact. If you receive a call like this, you should end it without providing any printer details. If you did provide printer information over the phone, please let ISG know.

For details on Brown's Office Equipment Program and its toner order directions, see: www.brown.edu/Facilities/Graphic_Services/services/svcs_copier_toner.html.

*More information:*
Examples from the Phish Bowl
http://www.snopes.com/crime/fraud/supplies.asp
http://www.techrepublic.com/article/teach-your-users-to-recognize-the-phoner-toner-scam/
http://www.consumer.ftc.gov/articles/0181-unordered-merchandise

*Variation:*
Fake Scanner Emails Infect Office Computers with Malware (8/21/2013)

Tags
Security