

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Overview
- The Scam
- Protecting Yourself
- Special Training Offer

The Tech-Support Phone Call Scam

GUEST EDITOR

Lenny Zeltser is the guest editor for this issue. Lenny focuses on safeguarding customers' IT operations at NCR Corp and teaches malware combat at the SANS Institute. Lenny is active on Twitter as @lennyzeltser and writes a security blog at blog.zeltser.com.

OVERVIEW

At the heart of many cyber attacks are criminals attempting to fool you out of your money or trick you into giving them your personal information. Common examples of this are fraudulent e-mails, called phishing, that pretend to come from a person or company you trust, such as your friend or your bank. While such e-mail attacks are still a threat, criminals are also calling potential victims on the phone. In this newsletter we explain how such a phone scam works, specifically a common tech-support scam, and what you can do to protect yourself.

THE SCAM

No two scams are ever exactly the same, however they often include many of the elements you are about to read here. You receive a phone call from a person claiming to be

from a computer support company associated with Microsoft or another legitimate company. They claim to have detected your computer behaving abnormally, such as scanning the Internet, and believe it is infected with a virus. They explain they are investigating the issue and offer to help you secure your computer. They then use a variety of technical terms and take you through confusing steps to convince you that your computer is infected, scaring you into ultimately buying their product.

For example, they may begin by asking you to download and install a program from their website or use online services that will give them remote access to your computer so they can troubleshoot and confirm the problem. These tools are usually legitimate remote access tools, such as LogMeIn.com or ShowMyPC.com, so they most likely will not be flagged by your antivirus software. With you on the phone, the scammer will then remotely walk you through various programs and settings on your computer. The person will attempt to convince you that he or she is taking actions to investigate the virus infection that is supposedly plaguing your computer. The caller may even begin to disable legitimate services that are always present on a

The Tech-Support Phone Call Scam

Windows computer, claiming the services are actually malicious programs. By disabling or even crippling your computer, they are attempting to scare you into believing that your computer is badly infected and the only way you can fix the problem is by purchasing their product or paying for an expensive annual subscription service. Their ultimate goal is to gain control of your computer, get your money, and potentially harvest your personal information.

Remember, everything these criminals are telling you is a lie; do not fall for such attacks. The reason criminals use the telephone instead of e-mail is that there is very little technology that can protect you from phone call scams like this. In addition, phone calls are a powerful way for criminals to convey emotion and a sense of urgency, thus increasing their chances of fooling you. The best protection from attacks like this is not technology, but yourself.

PROTECTING YOURSELF

At times legitimate companies whose services you use, such as your bank or your credit card company, may call you to confirm your account information, or to update you on a purchase. The challenge is determining when these phone calls are from legitimate companies and when they are scams. Here are some key steps to protect yourself.

- When someone asks you for information over the phone or asks you to take an action, be suspicious and confirm the person's identity first. Ask what company the person works for. If you have never heard of the company before, then there is a good chance this is an attack. If this is a legitimate company you know, then simply tell the person this



Be very suspicious of any caller asking for remote access to your computers or pressuring you to buy a computer security product, these phone calls are most likely a scam.

is not a good time for you to talk. Ask for a name and employee number and explain that you will call back. Then go to the organization's website or other information that you already have on file, get the phone number from there, and call the company back.

The Tech-Support Phone Call Scam

- If the phone caller is creating a sense of urgency or creating tremendous pressure for you to take action right away, this is most likely a scam. Do not trust them.
- Do not rely on Caller-ID alone to authenticate a caller. It is easy for criminals to spoof the Caller-ID or create fake Caller-IDs so they can pretend to be calling from a legitimate company when they really are not.
- Never give your password over the phone. No legitimate organization will ever ask you for your password.
- Never give an organization information they should already possess. For example, if your bank is calling you, the caller should already have your account number.

RESOURCES

Some of the links have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

Recording of Actual Tech-Support Scam:

<http://preview.tinyurl.com/cbg9kku>

Microsoft On Tech-Support Scams:

<http://preview.tinyurl.com/cxpwk9>

Symantec on Tech-Support Scams:

<http://preview.tinyurl.com/244raev>

Reporting Scams:

<https://www.ftccomplaintassistant.gov>

ISC Survey on Tech-Support Scams:

<https://isc.sans.edu/reportfakecall.html>

Common Security Terms:

<http://preview.tinyurl.com/6wkpae5>

SANS Security Tip of the Day:

<http://preview.tinyurl.com/6s2wrkp>

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at <http://www.securingthehuman.org>

SPECIAL PROMOTION

Does your Small or Medium organization need help with securing the most vulnerable part of your organization? Check out a great program to train up to 750 Users for just \$3,000. Program runs only from June 01 to July 31, 2012. Learn more at: www.securingthehuman.org/programs/sme

OUCH! is published by the SANS Securing The Human program and is distributed under the [Creative Commons BY-NC-ND 3.0 license](http://creativecommons.org/licenses/by-nc-nd/3.0/). Permission is granted to distribute this newsletter as long as you reference the source, the distribution is not modified and it is not used for commercial purposes. For translating or more information, please contact ouch@securingthehuman.org.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Cara Mueller