Phishing Scams

Author: Brian Lisse

A phishing scam is not malware per se, but often the end result is that your system becomes infected by malware. Phishing scams can be an email, phone call, or popup at a website that induces you to take an action that allows others to infect your computer.

Types of phishing scams:

1. You get a phone call, email, or pop up from someone purporting to be from Microsoft telling you that they have detected a virus or problem with your computer. They tell you to go to a website and click a link to let them take remote control of your computer to "fix" the problem. This is a scam! Microsoft will never call you to tell you that your computer has a problem. They have no way of knowing and do not take remote control of your computer.

2. You get a phone call or email from your bank or your credit card. They tell you that they have detected a problem with your account and need you to verify personal account information, or that you should fill out personal information at a site or in an email. This is a scammer- Your bank or credit card has all the information they need from when you set up the account with them. They would never need you to tell them account numbers, birth dates, social security numbers, or anything. If you are in doubt, don`t take their phone number, just take an old bill and call the bank or credit card directly to ask them if there is an issue with your account.

3. You may be having an issue with match.com, ebay, Charter, TDS, AOL, yahoo, etc. and decide to do a Google or Bing search to call them and get help. Scammers take out websites and names close to the real name so you think you are clicking on the company you need help with, but you are not. They then tell you they need to take remote control of your computer to help you and wham, they embed malware and infect your computer.

4. **Romance scams:** If you think you have a web relationship with someone but you have never met them physically face to face, *and there will always bean an excuse why they can't*, it is usually a scammer. It doesn't matter if they send a picture, talk with you on the phone, etc. **Never send them a single dime of money.**

5. Help me emails from someone you know- Help, I am in (name a country) and lost my wallet. Please send me money so I can get home, buy a ticket, get out of prison, etc. This is almost always a scam where they got your email address from a friend or family member whose email account has been compromised. If in doubt, call the person and talk with them only.

There are many more examples of phishing scams, but in summary, never give out personal information over the phone or via email if anyone solicits it from you. Also, NEVER give remote control of your computer to anybody unless you know them or have a relationship with that person. Would you let a person in to your house who has a ski mask on because they said your family member (parent, spouse, friend, etc.) said you would help them? When you give remote control of your computer to someone, you are letting them in. It is one thing if you know me and call me up, I might say, OK, let me take remote control and see what is going on, but you know me, where I work, my voice, etc. Only let someone you absolutely trust take remote control of your computer, ever!