Voice + Phishing = Vishing

Submitted by Julie Fugett on Wed, 2008-07-02 20:49.

UPDATE:

Please be alert for SMS messages (also commonly referred to as "text messages" or simply "texts") arriving on your mobile phones. Users report receiving the following text message from "system(at)66fcu.org":

> For usual maintenance please confirm your 66 F.C.U. details by calling at xxx-xxx-xxxx.

A member of the IT Security Office staff "took one for the team" and dialed the number. He described the message on the other end as "very professional sounding. There was a voice prompt that told you to enter your credit card number in--all electronic." I was all set to post a recording of the prompts, but it looks like the Federal Trade Commission got to them first. Score one for the good guys!

Have a listen to the FTC's message:

If you do not use your phone for text messaging, we recommend working with your mobile phone provider to disable the text messaging features of your phone. You may also want to limit or block text messages that are e-mailed to your phone.

Managing text messages:

AT&T customers: http://mymessages.wireless.att.com/
Verizon customers: http://www.vtext.com
Sprint customers: How do I block text messages?

If you have another mobile provider and can supply us with a website where users can manage their text message preferences, please pass it along.

Many thanks to Boone Bradley for his assistance with this update.

If you live in Lawrence or the surrounding area, there's a good chance you've gotten a phone call that sounds something like this in the last two to three days:

> Hello. This is a message from 66 Federal Credit Union. *(It may say KU Credit Union --Ed.)* Your Visa debit card has been suspended. To activate your card, please call the security department at *phone number redacted*.

You can also listen to a sample of the message below. For security reasons, the telephone number has been removed from the recording.

The calls may come along with Caller ID information, or they may say "Unknown Name/Unknown Number." The callback numbers given by the vishers vary and do not seem to be consistently located in any particular exchange or area code.

Here are the most frequently asked questions the IT Security Office has received regarding these calls:

How did they get my number?

> We believe the vishers are engaging in a practice known as war dialing. (If you'd like to see an entertaining example of wardialing, rent the movie WarGames.) The attackers dial numbers sequentially until they get an answer, then their message plays. It doesn't matter that you don't publish your number--they'll hit it eventually just by dialing every number in order.

What can I do to stop this?

> In two words? Not much. These people don't respect things like Do Not Call lists, and they are spoofing or not including their Caller ID information so they cannot be blocked by number. Your best bet is to screen your calls. If you do not recognize the number or no Caller ID data is present, let it go to the machine.

I got one of these calls. What should I do?

> It would be very helpful to us if you would pass along as much information about the call as possible. Send an e-mail to abuse@ku.edu with the subject line "vishing phone call" with the following information:
>
> 1. Time and date of the call
> 2. Any available Caller ID data
> 3. The financial institution named in the call
> 4. The callback number given in the call
>
> Alternately, you can file a complaint with the Internet Crime Complaint Center, which is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA).

Should I call them back just to be sure?

> NO.
>
> You should NEVER call a number left for you in a message like this. ONLY call known-good numbers like those printed on the back of your credit or debit cards.

Oh no! I called back and gave them my information. What should I do?

> Move quickly, but don't panic. Contact your financial institutions right away to alert them so that they can close your accounts, deactivate your credit/debit cards, and move all of your financial assets to new accounts. You may also wish to file a police report, and you should definitely file fraud alerts with the "big three" credit reporting agencies: Experian, Equifax, and TransUnion. The Federal Trade Commission has an excellent website devoted to recovering from identity theft. You may also wish to visit the KU Privacy Office's website on identity theft.

If you have further concerns, please do not hesitate to contact the KU IT Security Office. You may also wish to contact the Internet Crime Complaint Center, the Federal Trade Commission, and the financial institutions with which you do business.

Related reading...

Please do not click here to verify your KU account.
Look out! Fraudulent KU Credit Union e-mails on the loose!
The anatomy of a phish.
KU Credit Union phishing messages from ku.edu accounts

Fraudulent KU Credit Union e-mails

» login or register to post comments