A variant on phishing is “vishing”, which uses telephone systems to obtain information from unwary consumers. The term vishing is a combination of voice and phishing. Vishing is the criminal practice of using social engineering and Voice over Internet Protocol (VoIP) telephone systems to gain access to private personal and financial information from the public for the purpose of financial reward.

Consumers are becoming more aware that any email they receive containing a link or other contact information could be malicious in nature. So, criminals are using methods victims are more familiar with, like calling a number. Vishing exploits the public’s trust in telephone services, which have traditionally terminated in physical locations, are known to the telephone company, and are associated with a bill-payer. The victim is often unaware that VoIP allows for Caller ID “spoofing” and thus provides anonymity for the criminal caller. Vishing is attractive to criminals because VoIP service is fairly inexpensive, making it cheap to make fake calls. In addition, because it’s web-based, criminals can use software to create phony automated customer call center service lines.

An example of a vishing scam is when a consumer receives a recorded message telling them that their credit card and/or financial institution account has been breached and to immediately call a number provided in the recorded message. The phone number provided in the message leads the consumer to a fraudulent call center established by the perpetrator of the fraud. The perpetrator then attempts to obtain confidential account information and login credentials in order to access the account. A twist on this scam is when the recorded message provides the address of a fraudulent website for the consumer to access (instead of a telephone number) and to provide certain information to reinstate the supposedly affected account(s).

Vishing is very hard for authorities to monitor or trace. To protect yourself, we advise that you be highly suspicious of messages (telephone, email, or otherwise) directing you to call and provide personal, confidential, and/or account related information. Rather than provide any information, you should contact your financial institution or credit card company directly to verify the validity of the message (i.e. do not use contact information provided in the suspicious message).