Vishing - The Latest Cyberscam

August 28, 2020 - There is a good chance that you've never heard the term Vishing, but as the name implies, it is closely related to phishing. The big differences are that the crooks behind Vishing tend to be well educated about their target victims, and they contact those victims by voice calls. Now, you may be thinking, "I'd never fall for something like that!" But there are a variety of reasons that you could be completely wrong about that.

Vishing has risen out of COVID 19 and that fact that millions of people have started working from home. No longer can you easily verify that the person you are speaking with over the phone is actually someone who works in your office. That sort of face to face contact, where you can actually see the person's badge or know that they have access to your office, has gone out the window. Criminals know this and they are taking advantage of it in ways that you've probably never thought of.

One of the most dangerous ploys comes in the form of fake help desks. You receive an official call from someone pretending to be working in your company's IT department on the help desk. You're told that due to an upgrade, or some other similar thing, you will be receiving an email message to reset your password and other credentials.

The most frightening thing about the call - although you don't realize it at the time - is that the person on the other end of the phone knows who you are. They already know your name, your job title, who you report to, your job responsibilities, what office you work out of and quite likely the names of other people you work with. And you won't need to give them your email address. They already have that too. That's because they have done their homework. They looked at your LinkedIn profile as well as anything they could find on Facebook or other social media sites. They aren't running some phishing scheme headquartered in Nigeria. The person on the other end of the phone is polished, sounds educated and going for much bigger game. Duping you into buying a $500 gift card isn't the goal.

Their main focus is gaining access to your company's network. Shortly after the call, you receive an email message that looks just like it came from your company. Same letterhead. No misspellings. Good grammar. And it contains the link that was mentioned in the call. When you click on it, you're taken to a page that looks like your company's network. And if you go beyond this point, you give away the keys to the kingdom. You enter your credentials for logging onto the network and the person you were talking to now has access to it.

An attack like this can be more damagingâ€¦ much more damagingâ€¦ than malware or other scams. If your company has multiple networks, or multiple levels of security, depending upon the information you reveal, you could be giving criminals

complete access. That means access to bank accounts, personnel information, suppliers, etc. You may have just given it all away, jeopardizing both the company and everyone who works for it. You get the idea.

One of the biggest issues with Vishing is that there is no easy solution to protect yourself from it. Since it isn't software based, your antivirus and malware solutions really can't help. And since just about everyone has an online profile these days, there is no easy way to keep someone from researching you or your employees. About the only thing that you can do is put in place policies to deal with this type of scenario. But in order for those policies to work, you would need to give them some teeth. For instance, violating this policy is grounds for immediate termination. Something like that.

Companies with help desks should have specific help desk policies. Something like, we will never call you and ask you to make a change over the phone or via email. Put together procedures for communications and follow them. That's true for companies without a help desk too. And it's the only way that you're going to be able to protect yourself from schemes like this.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS