Whenever we receive a call from an unknown number, we are unaware of the person on the other end. It is in situations like these that a person can become a victim of vishing. A vishing scam is a form of phishing in which the person on the other end scams you to get your personal information. These malicious people act like someone from a trusted source and use social engineering hacks to get your information. Vishing is present in any form of communication: calls, messages, or email.

## How to identify vishing scams?

Some loopholes can give you a clue that you are becoming a victim of vishing:

### IRS, Medicare, Social Security Administration

None of the federal agencies mentioned above will ever contact you on their own unless you try to contact them. Thus, if you ever get a call or message from one of the federal agency administrators, you should be cautious because it can be a vishing scam.

### Threats of urgency

In many cases of vishing scam, the hacker presents you with a tense situation that you will have to face severe consequences if you do not provide the information instantly. You might also hear of threats like immediate arrest, blockage of accounts, or a high amount of fine.

### Information to start

Sometimes the vishing scammer has some basic information about you to trick you into providing the rest of the information.

## How to prevent vishing scams?

There are always a bunch of solutions to counter a problem:

### Verify calls

If you receive an unexpected call, then the first thing you should do is verification. Do not immediately provide your information, instead hang up on the call and verify if the number is authentic. You may use an official directory for this purpose.

### Be vigilant

Official organizations such as banks do not call their users and ask them for login credentials. If you receive any call of such type, then beware because it acts as the vishing scammers.

### Beware of unexpected links

When vishing scammers try to seize your information through emails, they may send a link. However, do not click on such unexpected links.

### Don’t respond to prompts

Another form of vishing scams is the automated messages, which ask you to press a certain number or say a specific word. Scammers may use this data to access your private accounts.

## Conclusion

As technology is advancing, hackers are also finding new ways to get hold of your information. Thus, you should learn how to prevent yourself from situations like vishing scams.