7 Ways to Avoid Becoming a Victim of Vishing

Social engineering via phone call is called voice phishing or "vishing". Unlike other attacks to hack into people's computers or accounts, there are fewer security technologies that can detect and prevent a phone call attack; also, it is much easier for criminals to convey emotion and build trust over the phone, which makes it easier to trick their victims. Here are 7 ways to avoid becoming a victim:

1. **Be suspicious of anyone who calls you and creates a sense of urgency or pressure.** They are attempting to rush you into making a mistake like providing information, turning over control to your device or making a fraudulent purchase. If a call starts to feel strange, stop and say no.

2. **Do not purchase gift cards or prepaid credits cards over the phone.** If anyone insists that you purchase gift cards or prepaid credit cards, this is a scam.

3. **Caller ID can be misleading.** Bad actors can spoof the number, so it looks like it is coming from a legitimate organization.

4. **Do not allow a caller to take control of your computer.** Never allow a caller to take temporary control of your computer or trick you into downloading software. This is how they can infect your computer.

5. **Do not give the caller informtion they should have.** Unless you placed the call, do not give the other party information that they should already have. For example, if your credit union called you, they shouldn't be asking for your account number.

6. **If you believe a phone call is a scam, simply hang up.** You can then go to the organization's authentic website and call the customer support phone number directly yourself.

7. **Let unknown calls go to voicemail.** If a phone call is coming from someone you do not personally know, let the call go directly to voicemail. This way you can review unknown calls on your own time.

sovereign® INSURANCE