Scam of the Week: Working From Home? Don’t Fall for This “Phony” Call

The Coronavirus Disease 2019 (COVID-19) pandemic has caused a massive shift in the number of employees who are working remotely. From a cybercriminal’s perspective, this is a perfect opportunity for their social engineering scams.

One scam involves cybercriminals calling you and posing as support personnel from the companies or services that your organization may be using to allow you to work remotely. Typically, the caller will try to gain your trust by stating your job title, email address, and any other information that they may have found online (or on your LinkedIn profile). Then, the caller claims that they will send you an email that includes a link that you need to click for important information. Don’t fall for this scam!

Remember the following to help protect yourself from these types of scams:

- Never provide your personal information or work information over the phone unless you’re the one who initiated the call.
- Scammers can spoof any number they’d like. Therefore, even if a call looks like it’s coming from a legitimate source, it could be a scam.
- If you receive this type of call, hang up the phone immediately and notify the appropriate team in your organization.

Stop, Look, and Think. *Don't be fooled.*
The KnowBe4 Security Team
KnowBe4.com