Vishing

What you should know about it:

In vishing, a cybercriminal contacts you by phone, impersonating someone in a position of authority. Vishing is similar to phishing, but the attack is delivered by phone instead of via email.

The caller might pretend to be from the company's IT or finance department, impersonate an executive or business partner, or claim to be from a software company such as Microsoft. The caller attempts to convince you to provide private information or take an action that can be used to compromise the company's systems, or to steal from you personally.

How to safeguard against it:

- **Verify unexpected phone requests in ways that aren't connected to the incoming phone call. For example, use an official directory and another phone to call the company's main office and ask to speak with the caller who is making the request.**
- **Be very suspicious of any caller who asks you to share login information over the phone.**
- **If a caller asks you to provide account data or personally identifiable information, refuse to do so — and report the contact to security.**
- **Security won't call you to request that you change logins, passwords, or network settings. Any caller who makes this type of request is probably a scammer. Refuse the request and notify security.**