Security Hints + Tips — Pretexting

May 6, 2024

Pretexting is when the bad guys create a false scenario using a made-up identity or pose as someone you know. They can even pose as employees of bank or credit card companies to manipulate you into divulging personal or sensitive information.

How it Works: Common Tactics of Influence

The bad guys will try to persuade you into giving them sensitive information. Oftentimes, the information that they need is not specific to your organization. Below are examples of two common tactics used to influence victims in pretexting scenarios:

Pretexting with Authority

You receive a call at work from someone demanding immediate assistance. They are speaking in an aggressive and authoritative tone. This person establishes their authority by using an executive-level or official-sounding job title. They may even insult you for not being familiar with "who they are". These scare tactics often persuade victims into giving away sensitive information or complying with the cybercriminal's request. It's human nature to act in a responsive manner around someone of authority, but don't fall victim to false claims of authority!

Pretexting with Obligation

You receive a call from someone posing as a member of your IT department. The bad guy tells you they've found malicious activity on your work computer and begin questioning your recent browsing history. The fake IT employee implies that you've accessed a malicious website and have put the company in danger as a result. They demand you update your password with a more "secure" password which they provide. Would you feel obligated to comply with their instructions? Many unsuspecting people would, but don't fall victim to a false sense of obligation!

How Can I Avoid Falling Victim to Pretexting Scenarios?

Use the tips below to help protect your organization against pretexting scenarios:

Never give out sensitive information over the phone, online, or in email, unless you are absolutely sure you know who you're dealing with, or you initiated contact with the individual.

If the caller claims to be an employee but their request seems suspicious, verify their identity through a trusted party and let them know you'll call them back. If the caller questions the need for your verification efforts, explain that you're following the process required for sharing the type of information they are requesting. Maintain a respectful but forceful attitude.

Make sure you're familiar with your organization's protocols for handling requests for information or ask your supervisor if you need assistance.

The KnowBe4 Security Team
KnowBe4.com


KnowBe4
Human error. Conquered.