Cyber Hygiene: Pretexting Scams

Social engineering schemes are designed to fool their target (you) into giving away private data. While phishing tends to be the most well known style, pretexting is on the rise.

Understand the Scam:

What is pretexting?

A scammer attempts to build a connection in one of two ways: impersonate someone you know, such as a coworker, or fabricate an identity of a worker from a trusted company. This style of scam involves time and research of their target in order to make an accurate connection and build trust.

How do they scam you?

The scammer identifies themselves as a company representative, gains your trust and then asks for the information they are looking for. Believing you are talking to a real representative, you willingly give them the information they want.

How is it being used?

Legitimate professions such as sales people and law enforcement use this technique to make better sales or elicit information they need to solve a case. The difference is in the intent of their inquiry.

An IT representative calls you saying there have been small breaches on company computers. He needs to remotely access your computer to ensure all cybersecurity protocols are in place on your company device. Since everyone is working remotely, he can't have you bring your device in, which is normal procedure, so this is the next best option. You give him your IP address and he has access to control your computer. You see random windows beginning to pop up and realize too late he is stealing your information.

Learn to defend yourself:

Limit social media posts

For these scams to work, cybercriminal must research their target. The more information you post online, the easier it is for them to learn how to best scam you.

Cyber Tip: Supporting 2020 seniors by posting your own graduation picture is nice, but be wary. School names and mascots are often answers to common security questions.

Go to the source

If a representative from a company contacts you in person, on the phone or via email, verify their identity directly with the company. If someone comes to your house claiming to be with a company, find the corporate number on your own and

Never give out personal info

Real company representatives will never ask for your password, full account numbers or credit card numbers. General conversations that steer in a personal direction should be politely ended.

"Thank you for asking but I would rather not talk about my... children, work, family."

Protect your organization

Do not give out company information, even if the requester appears to be from within the company. Know your company's procedures for proper communications when there is an issue, or the company needs information from you.

CyberCompass®
SECURITY

CyberCompass navigates businesses to cyber resilience across their business ecosystem of their people, processes, technology and vendors. We are a one-stop solution for a cybersecurity, compliance and privacy program.