OUCH! July 2023

The Monthly Security Awareness Newsletter for You

Stop Those Phone Call Scams

The Story

David was busy watching his favorite streaming series when he got a phone call from a number he did not recognize. The area code was the same as his, so he assumed it was someone local and answered the phone. Right away David was asked to confirm his full name. The caller then stated that he was from the police department and that a warrant had been issued for David's arrest. David's taxes were outstanding and if they were not paid in the next 24 hours, the police would have to arrest him. David was terrified and asked what he needed to do.

The caller then gave him the phone number of the local government tax department where he could take care of the outstanding taxes. David immediately hung up and then called that number, which was answered by a kind lady who identified herself with the local tax department. David gave her his full information. After a moment, she confirmed that he had $1,487.72 outstanding in taxes. If he paid immediately over the phone with his credit card, she would be able to take care of the situation and he would not go to jail. David was relieved and immediately gave her the credit card information, which she charged for the full amount, telling him everything was resolved.

The Attack

The problem was that the callers were neither from the police department nor a government tax agency. These were two criminals working together to scam people. They were calling thousands of random people and repeating the same story. They used special software to ensure that the number they called from always used the same area code as the victims they were calling, making it look like their phone number was local and more trusted.

These criminals use other stories as well — everything from claiming that your warranty has expired, to providing business loans you can take out for free, to fixing your infected computer. Quite often they are trying to get your credit card information or passwords, fool you into transferring them money, or perhaps even give them remote access to your computer.

These scammers often create a tremendous sense of urgency or promise you something too good to be true in order to trick you. They use emotion to rush you into making a mistake. They may have also collected prior information about you which they'll use to establish credibility.

More recently, with the availability of artificial intelligence services, scammers can even change their voices in phone calls.

The Counterattack: What You Can Do

There are several steps you can take immediately to protect yourselves:

- Configure your phone to only allow calls from trusted numbers in your phone's Contacts or Address Book. This makes it so that any call from someone you do not know will instead go directly to voicemail. The vast majority of scammers will not even bother leaving a voice message, and for the ones who do, it is easier to determine if it's a scam and delete. In addition, some service providers also have call screening service which you can enable.

- If you do end up on the phone with someone you do not know, be cautious. If they are pressuring you into taking an action, it's most likely a scam. If they say it's your bank calling, hang up and use a trusted phone number to call your bank back, such as the number on your bank card. If they say it's the government calling, go to that government department's website and find a trusted phone number to call back. The longer they have you on the phone, the more likely they can trick you.

- Never provide the caller with personal or sensitive information that they should already have. If your bank calls you, they should already know your name, address, and account number.

Modern scammers are extremely aggressive. They have nothing to lose and everything to gain. Configure your phone to only receive phone calls from contacts you know and trust, and when in doubt, hang up!

Guest Editor

Prajakta Jagdale is Sr. Director of Offensive Security and Incident Command at Palo Alto Networks. She serves as a member of the Board of Directors of Women in CyberSecurity. She is passionate about all things security, including workforce diversity. Linkedin: https://www.linkedin.com/in/prajaktajagdale/.

Resources

Emotional Triggers: How Cyber Attackers Trick you: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Only allow calls from your contacts

Android: https://support.google.com/fi/answer/12982560?hl=en&co=GENIE.Platform%3DAndroid#
Apple: https://support.apple.com/guide/iphone/avoid-unwanted-calls-iphe4b3f7823/ios