RICHTER GUARDIAN

RGSA 08-30-23-01
Date:August 30, 2023

Protecting Against Technical Support Fraud

INTRODUCTION

Cyber criminals have been carrying out technical support scams for over a decade. As technology evolves, so do the techniques of fraudulent tech support scammers, making it difficult for people to discern whether the technical support team they're speaking to is legitimate. Technical support scams are so common that the FBI's Internet Crime Report of 2022 reported that 'Tech Support Crime' had over 30,000 recorded victims in 2022.

SUMMARY

Technical support scammers use many different techniques to trap people and gain access to their computers and other devices. After they convince you that there is a problem, they request an exorbitant fee in return for their help. Here are two of the most common methods technical support scammers use to trick their victims:

1. Phone calls, emails and text messages – Technical support scammers may call, email or send a text message and pretend to be a computer technician from Apple, Microsoft, or any well-known technology company. They will assure you that there is a problem with your computer, and request that you give them remote access to your computer to help remediate the issue.

2. Pop-up warnings – Technical support scammers may trick you with pop-up windows; it may look like an error or warning message from your device, and it may use similar graphics from trusted websites. The pop-up will often provide a phone number that you can call to get help. The phone number will lead to a fraudulent tech support worker.

RECOMMENDATIONS

1. Stay Informed – Always be skeptical of unsolicited calls, emails or text messages that report a problem with your device.

2. Prevent Remote Access – When a technical support scammer has you on the line, they will convince you to provide them remote access to your device in order to run diagnostic tests. Do not provide remote access to your device.

3. Trust Your Instincts – If you are suspicious about an unexpected message, call, or request for personal information or money, it is safe to assume it may be a scam.

4. Stay Educated – Participate in security awareness sessions provided by your Richter Guardian team, your bank or other trusted organizations.

HOW RICHTER GUARDIAN CAN HELP YOU

We understand that misleading pop-ups or warnings about your device through a call can cause uncertainty. Richter Guardian's monitoring system and concierge service can give you peace of mind. Your onboarded mobile and endpoint devices are monitored by us. If there is a problem with your device, we will contact you to provide specific details about any potential alerts. Our experts can help you remediate the issue.