FRAUD AWARENESS

Tech Support Scams

Creating a sense of urgency, tech support scammers pose as technical support representatives from well-known companies, such as Microsoft and others, to contact individuals claiming that their computer has a virus or other technical issues. They aim to gain remote access to the victim's computer or extract money for fake services. Below is a list of common tech support scams that you should be aware of:

Phone Calls: Scammers pose as computer technicians from well-known companies, aiming to gain unauthorized, remote access to your computer. Once inside, they use fake diagnostic tests to convince you to pay for nonexistent issues.

Pop-Up Warnings: In this scam, a deceptive pop-up message claims there's a security problem on your computer. The message, which may contain an actual company's logo and appear to be legitimate, is designed to resemble an error notification from your operating system or antivirus software, prompting you to call a specified number to address the issue.

Emails: Scammers send emails that inform you of an account suspension and provide a link to resolve the issue. Clicking the link, however, results in the installation of a virus on your computer, allowing the scammer access to your system.

Online Ads and Search Results: Scammers invest in paid search advertising to promote their fake tech support services. When you call, they impersonate well-known companies, convincing you to pay for their services while potentially stealing your information, either over the phone or through malicious software.

How to protect yourself from these scams:

- Refrain from granting control of your computer to unfamiliar individuals, whether through email or phone calls. Avoid sharing your personal information or allowing access to your computer.
- Do not click on links within unsolicited pop-ups or emails. These links often contain malicious viruses designed to steal your information.
- Install and regularly update your antivirus software to enhance your computer's security.
- Recognize that legitimate tech companies do not typically reach out via email, text messages, or phone calls to notify you about computer security issues. Be cautious when such communication occurs.

Remember, it's important to safeguard your online security by not allowing strangers access, protecting your computer against viruses, and not falling prey to unfamiliar phone and email solicitations that may request computer access through suspicious links or by gathering your personal information.

To report a tech support scam, visit **ReportFraud.ftc.gov**.

BankFinancial℠

1.800.894.6900 | BankFinancial.com