Morgan Stanley

Tech Support Scams

Fraud artists are savvy and can be very convincing. The Tech Support Scam is a popular social engineering technique, with several twists.

How Tech Support Scams Work

Vishing

1. You get a call from someone claiming to be from a major company.
2. They tell you there's a problem with your computer, such as a virus.
3. They request remote access to your machine to perform a diagnostic test.
4. They ask you to send an urgent payment via wire transfer or prepaid gift card to fix the issue.

Scareware

1. While online, you get an alarming pop-up warning you about an urgent security matter.
2. The message contains a reputable company's logo, so it appears legitimate.
3. The message instructs you to click a link for more information or to pay for and download an antivirus product.

If you comply to the requests made in either variation of this scam, you could not only lose money, but also make your devices and information stored on them available to the scam artist.

In the unfortunate event that you fall victim to what you believe to be a Tech Support Scam, responding quickly can help limit the damage.

Action Steps

1. If you provided financial account information, immediately contact your financial institutions and discuss cancelling fraudulent charges, obtaining a new credit/debit card or opening a new account.

2. If you unwittingly downloaded "scareware" onto your device or granted remote access to your computer, seek the help of a trusted expert to have any malware removed or uninstalled.

3. Visit IdentityTheft.gov for more information and specific actions to take based on your situation.

Tips and Best Practices

DO hang up on unsolicited callers and call a phone number listed on the company's official website.

DON'T give out any personal information on the phone, especially if you did not initiate the call.

DO use strong, unique passwords for your accounts and enable multi-factor authentication wherever available.

DON'T pay for services with gift cards or money transfer apps.

DO ensure your device's operating system, browsers and software are up to date and that you've done your research about any antivirus product you're using.

DON'T click on any links, provide any information or make payments on websites that pop-up. Consider enabling pop up blockers.

DO report the incident to the Federal Trade Commission at ReportFraud.ftc.gov.

DON'T provide remote access to your computer or account log-in information, such as your username and password.

Sources:
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.
https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams.
https://us.norton.com/internetsecurity-online-scams-how-to-spot-online-scareware-scams.html.
https://www.pcmag.com/how-to/how-to-avoid-scareware.

WM10122103 CRC# 3908711 02/2025