NORTH DAKOTA STATE AND LOCAL INTELLIGENCE CENTER

Tech Support Scams

What are tech support scams?
Tech support scams are a type of social engineering attack where cybercriminals pose as legitimate tech support from well-known companies (e.g., Microsoft, Apple, Google, or Geek Squad) to deceive victims. These scams often start with a phone call, a pop-up warning on the screen, or a fake ad, alerting users to a supposed virus or critical issue with their computer. The attackers usually ask the victim to grant remote access to their device. These scams rely heavily on creating a sense of urgency, convincing victims that immediate action is needed to avoid severe consequences like data loss or identity theft.

Who do tech support scams target?
IT support scams primarily target less tech-savvy individuals, home users, small businesses, and those actively seeking technical assistance online. These scams often exploit people's lack of familiarity with IT systems, creating a sense of urgency by claiming that a device is infected or malfunctioning. Older adults may be more vulnerable, as well as individuals already experiencing technical issues or frustration. Small businesses without dedicated IT support may also fall victim to these scams, as scammers impersonate legitimate tech companies and offer "solutions" to their IT problems.

What do tech support scams target?
IT support scams primarily target sensitive personal information, financial details, and access to victims' devices. Scammers generally aim to gain remote control over a device allowing them to steal data such as passwords, banking information, and personal documents. In many cases, they hope to install malware which can further compromise a victim's system. Scammers frequently demand payment for unnecessary or fake services often through credit cards or untraceable methods like gift cards or cryptocurrency.

How do I protect myself?
Do not grant remote access to a computer unless you are certain they are a legitimate tech support professional you already do business with. Even if you are familiar with the source if the request for remote access is unexpected verify with their known and official contact info before proceeding.

Ignore unexpected phone calls, emails, or pop-up messages claiming to be from tech support. Legitimate companies rarely reach out directly about technical issues. Legitimate tech support will not ask for personal details, passwords, or payment for services you did not initiate.

Share knowledge of these scams with family, friends, and colleagues, particularly those less familiar with technology, so they can recognize the signs and avoid falling victim.

ndslic@nd.gov