DISB
Government of the District of Columbia
Department of Insurance, Securities and Banking
Consumer Alert

# Tech Support Scams

The District of Columbia Department of Insurance, Securities and Banking (DISB) is warning District consumers to be on the alert for tech support scams.

**What Is a Tech Support Scam?**
Someone contacts District residents by telephone, email, computer pop-up advertisement, or text message pretending to be a representative or technical support person from a software company like Apple or Microsoft.

Scam artists will use scare tactics to try to convince you that your computer has a serious problem or is vulnerable to attacks. They may claim that:

- Your antivirus or firewall protection has been turned off;
- Suspicious activity has been detected on your network; or
- A third party has hacked your computer network.

The fake tech support specialist will ask you to grant them remote access to your computer and then pretend to run a diagnostic test. After running the test, they will claim there are problems with your computer and it has been infected by a virus or malware. The scammer will offer to repair the problem for a fee that you can pay by sharing your credit card, debit card, or gift card information.

**Things You Should Know**
Once the fake tech support specialist gains remote access to your computer, they can steal your financial and personal information and any other data you may have stored on the computer. Also, the scammer can install software that grants them continued access to your computer system. This means your computer was hacked—someone has unauthorized access to your computer system and your information.

**Avoid Becoming a Victim**
If you receive a telephone call, email, or text message from someone pretending

to be from Microsoft, Apple or some other software company telling you that your computer has been infected by malware, hacked, or its security is disabled, hang up the phone and do not respond to the email or text message. Never provide your personal or financial information to anyone you do not know. Also, never give anyone you do not know and trust remote access to your computer.

Legitimate software and tech support companies will never:

- Send unsolicited emails or text messages;
- Make unsolicited telephone calls requesting your personal and financial information to repair your computer; or
- Create security pop-up warnings that ask you to click on them to have your computer repaired or call a phone number.

If you believe you have been a victim of a tech support scam or have questions, contact the Federal Trade Commission's Consumer Response Center at 1-877-FTC-HELP (1-877-382-4357). You may also contact DISB's Enforcement and Consumer Protection Division at 202-727-8000.

Learn how to avoid other scams by visiting disb.dc.gov/page/consumer-scams.

*Issued: March 3, 2020*